ON NONLINEARITY AND GLOBAL AVALANCHE CHARACTERISTICS OF VECTOR BOOLEAN FUNCTIONS

WANSOON KIM* AND HEE-SUNG HWANG

Abstract. It is well known that the nonlinearity of vector Boolean functions $F$ on $n$-dimensional vector space $GF(2)^n$ to $GF(2)^m$ is bounded above by $2^n - 1 - 2^{\frac{n}{2}} - 1$. In this paper we derive upper bounds and a lower bound on the nonlinearity of vector Boolean functions in terms of auto-correlations. Strengths and weaknesses of each bounds are examined. Also, we modify the notions of the sum-of-square indicator and absolute indicator for Boolean functions to the case of vector Boolean functions to measure global avalanche characteristics of vector Boolean functions. Using those indicators we compare the global avalanche characteristics of DES(Data Encryption System) and Rijndael.

AMS Mathematics Subject Classification : 94A60
Key words and phrases : Nonlinearity, global avalanche characteristics

1. Introduction

Three of the most important criteria for cryptographically strong Boolean functions are balancedness, nonlinearity and propagation criterion. We call a Boolean function is a balanced function when input coordinates of a Boolean function are selected independently at random the output of the function must behave as a uniformly distributed random variable. On the other hand, the nonlinearity of Boolean functions measures the ability of a cryptographic system using the functions to resist against being expressed as a set of linear equations. The nonlinearity of a Boolean function $f$ on $GF(2)^n$ is the minimum hamming distance between $f$ and all affine functions on $GF(2)^n$. One often wishes to find out the nonlinearity of a cryptographic function, or when the exact value is not easily obtainable one wants to estimate the nonlinearity using extra information

Received December 5, 2003. * Corresponding author.
on given Boolean functions. Zhang and Zheng [6] obtained upper bounds and lower bounds on the nonlinearity using the notion of auto-correlation. The first aim of this paper is to extend the notion of auto-correlations of Boolean functions to vector Boolean functions and obtain the upper bounds and a lower bound on the nonlinearity of vector Boolean functions in the context of auto-correlations. Strengths and weaknesses of each bound are also examined. This result generalizes Zhang and Zheng’s results [6].

A Boolean function on $GF(2)^n$ is said to satisfy the propagation criterion with respect to a nonzero vector if complementing input coordinates according to the vector results in the output of the function being complemented 50% of the time over all possible input vectors, and to satisfy the propagation criterion of degree if complementing or less input coordinates results in the output of the function being complemented 50% of the time over all possible input vectors. A function is considered to have good avalanche characteristics if it does not have a nonzero linear structure and satisfies the propagation criterion with respect to the majority of the vectors. The second aim of this paper is to extend the notion of global avalanche characteristics [7,8] for Boolean functions to vector Boolean functions.

Also we modify the notions of the sum-of-square indicator and absolute indicator for Boolean functions to the case of vector Boolean functions to measure global avalanche characteristics of vector Boolean functions. Using those indicators we compare the global avalanche characteristics of DES (Data Encryption System) and Rijndael.

2. Basic definitions and properties

In this section, we introduce notations, definitions and well known properties for cryptographic Boolean functions which will be used in this paper. Let $GF(2)^n$ be an n-dimensional vector space over the Galois field $GF(2)^n$. Put

$$GF(2)^{n^*} = GF(2)^n - \{0\}.$$ 

A function $f$ from $GF(2)^n$ to $GF(2)$ is called a Boolean function on $GF(2)^n$. Let $B_n$ denote the set of all Boolean functions on $GF(2)^n$. Let $f \in B_n$ be a Boolean function. The truth table of $f$ is a (0, 1)-sequence defined by

$$(f(a_0), f(a_1), \ldots, f(a_{2^n - 1}))$$

where

$$a_0 = (0, 0, \ldots, 0), a_1 = (0, 0, \ldots, 1), \ldots, a_{2^n - 1} = (1, 1, \ldots, 1).$$

The sequence of $f$ is a (1, -1)-sequence defined by

$$((-1)^{f(a_0)}, (-1)^{f(a_1)}, \ldots, (-1)^{f(a_{2^n - 1})})$$
where each exponent is regarded as being real-valued. Let \( a = (a_1, \cdots, a_m) \) and \( b = (b_1, \cdots, b_m) \) be two vectors (or sequences), the scalar product of \( a \) and \( b \) denoted by \( <a, b> \), is defined as the sum of the component-wise multiplications. In particular, when \( a \) and \( b \) are \((0,1)\)-sequences,
\[
<a, b> = a_1 b_1 \oplus \cdots \oplus a_m b_m
\]
where the addition and multiplications are over \( GF(2) \), and when \( a \) and \( b \) are \((1,-1)\)-sequences,
\[
<a, b> = a_1 b_1 + \cdots + a_m b_m
\]
where the addition and multiplications are over the reals. A function \( f \in B_n \) that takes the form of
\[
f(x) = a_1 x_1 + \cdots + a_m x_m
\]
where \( a_j, c \in GF(2) \), \( j=1,2,\cdots,n \) is called an affine function. Furthermore \( f \) is called a linear function if \( c = 0 \).

The Hamming weight \( W(x) \) of \( x \in GF(2)^n \) is the number of ones in \( x \). The Hamming distance between two functions \( f \) and \( g \) is defined by
\[
\#\{x | f(x) \neq g(x)\}.
\]
We denote it by \( wt(f + g) \). The minimal distance between \( f \) and any affine function from \( GF(2)^n \) into \( GF(2) \) is the nonlinearity of \( f \), that is,
\[
N(f) = \min_{\phi \in \Gamma} wt(f + \phi)
\]
where \( \Gamma \) is the set of all affine functions over \( GF(2)^n \). The nonlinearity of Boolean functions measures the ability of a cryptographic system using the functions to resist against being expressed as a set of linear equations. It is known that the nonlinearity of arbitrary Boolean function is bounded above by \( N(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1} \). A function with this maximal nonlinearity is called a bent function and exists if and only if \( n \) is even. The Walsh- Hadamard transformation of a Boolean function \( f \) is defined as
\[
W_f(a) = \sum_{x \in GF(2)^n} (-1)^{f(x) + <a,x>},
\]
for \( a \in GF(2)^n \). Since
\[
W_f(a) = wt(f(x) + <a, x>) - wt(f(x) + <a, x> + 1),
\]
we have
\[
N(f) = 2^{n-1} - \frac{1}{2} \max_{a \in GF(2)^n} |W_f(a)|.
\]
Since a bent function has the maximal nonlinearity \( 2^{n-1} - 2^{\frac{n}{2}-1} \), equivalently, a bent function is defined as a Boolean function with \( W_f(a) = \pm 2^\frac{n}{2} \) for all \( a \in GF(2)^n \).

Cryptographic applications, such as the design of strong substitution boxes, require that when input coordinates of a Boolean function are selected independently, at random, the output of the function must behave as a uniformly
A Boolean function $f \in \mathcal{B}_n$ is balanced if

$$\#\{x \in GF(2)^n \mid f(x) = 0\} = \#\{x \in GF(2)^n \mid f(x) = 1\}.$$ 

Both linear functions and affine functions are balanced functions.

A Boolean function $f \in \mathcal{B}_n$ satisfies the Strict Avalanche Criterion (SAC) if and only if

$$\#\{x \in GF(2)^n \mid f(x + a) = f(x)\} = 2^{n-1}$$

for any $a \in GF(2)^n$ with $W(a) = 1$. That is complementing a single bit results in the output of the function being complemented with a probability of a half. We say a Boolean function $f$ satisfies the propagation criterion (PC) with respect to a vector $a \in GF(2)^n$ if and only if

$$\#\{x \in GF(2)^n \mid f(x + a) = f(x)\} = 2^{n-1}$$

or equivalently $f(x + a) + f(x)$ is balanced. A Boolean function is said to satisfy $k$-th order propagation characteristic if is balanced for all $a \in GF(2)^n$ with $1 \leq wt(a) \leq k$. For a Boolean function $f$, if $f(x + a) + f(x)$ is a constant for $a \in GF(2)^n$, $a$ is called a linear structure of $f$. The following results can be found in [8].

**Lemma 1.** Let $\mathcal{B}_n$ be a Boolean function on $GF(2)^n$. Then the following statements are equivalent.

1. $f$ is bent.
2. $<\xi, l> = \pm 2^{\frac{n}{2}}$ for any affine sequence $l$ of length $2^n$, where $\xi$ is the sequence of $f$.
3. $f(x) + f(x + a)$ is balanced for any nonzero $a \in GF(2)^n$.

**Lemma 2.** Let $f$ be a bent function. Then the following holds.

1. $f$ satisfies PC of degree $k$ for all $1 \leq k \leq n$.
2. $f$ satisfies SAC.
3. $f$ has maximum nonlinearity.
4. $f$ has no linear structure.
5. $f$ is not balanced.

Given a Boolean function $f$ on $GF(2)^n$ and a vector $a \in GF(2)^n$, we denote by $\xi(a)$ the sequence of $f(x + a)$ . The Auto-correlation of $f$ with a shift $a$ is defined by

$$\Delta_f(a) = <\xi(0), \xi(a)>.$$
To further simplify our discussions, $\Delta_f(a)$ will be written as $\Delta_f(a)$ if the function under consideration is clear. Obviously, $\Delta(a) = 0$ if and only if
$$f(x) + f(x + a)$$
is balanced, and $|\Delta(a)| = 2^n$ if and only if
$$f(x) + f(x + a)$$
is a constant, i.e, $a$ is a linear structure of $f$. The following Lemmas show upper bounds and a low bound on nonlinearity of $f$ [6].

**Lemma 3.** For any Boolean function $f$ on $GF(2)^n$, the nonlinearity of $f$ satisfies
$$N_f \leq 2^{n-1} - \frac{1}{2} \sqrt{2^{2n} + 2^{n-1} \sum_{j=1}^{2^n} \Delta^2(a_j)}.$$  

It is easy to verify that the bound does not exceed the well known bound $2^n - 2^{n-1}$. In addition, as the equality holds if $f$ is bent, the bound is tight.

**Lemma 4.** For any function $f$ on $GF(2)^n$, the nonlinearity of $f$ satisfies
$$N_f \leq 2^{n-1} - \frac{1}{2} \sqrt{2^n + \Delta_{\text{max}}}$$
where $\Delta_{\text{max}} = \max\{|\Delta(a)||a \in GF(2)^n\}$.

**Lemma 5.** For any function $f$ on $GF(2)^n$, the nonlinearity of $f$ satisfies
$$N_f \geq 2^{n-2} - \frac{1}{4} \Delta_{\text{min}}$$
where $\Delta_{\text{min}} = \min\{|\Delta(a)||a \in GF(2)^n\}$.

### 3. Upper bounds and a lower bound of nonlinearity of vector Boolean functions

In this section, we introduce vector Boolean functions. Also we introduce the notion of auto-correlation and derive upper bounds and a lower bound of nonlinearity vector Boolean functions in terms of those notions.

A function $F : GF(2)^n \rightarrow GF(2)^m$ is called a vector Boolean function on $GF(2)^n$. When $n \leq m$, $F$ is said to be balanced if and only if
$$\{x \in GF(2)^n | F(x) = b\} = 2^{n-m}$$
for any $b \in GF(2)^m$. Note that if a basis of $GF(2)^m$ over $GF(2)$ is specified, there are unique boolean functions $f_i$’s such that $F = (f_1, f_2, \cdots, f_m)$. We denote by $b \cdot F$ the Boolean function

$$b_1f_1 + b_2f_2 + \cdots + b_mf_m$$

for $b = (b_1, b_2, \cdots, b_m) \in GF(2)^m$. The nonlinearity of $F$, $N(F)$, is defined as

$$N(F) = \min_{b \in GF(2)^m} N(b \cdot F) = \min_{b \neq 0, \phi \in \Gamma} \text{wt}(b \cdot F + \phi)$$

where $\Gamma$ is the set of all affine functions over $GF(2)$. It is known that the nonlinearity of arbitrary vector boolean function is bounded above by $N(F) \leq 2^n - 1 - 2^{rac{n}{2}} - 1$. A function with this maximal nonlinearity is called a bent function and exists if and only if $n \geq 2m$ and $n$ is even. Equivalently, a bent function can be defined as a Boolean function with $W_{b,F}(a) = \pm 2^{rac{n}{2}}$ for all $a \in GF(2)^n$ and $b \in GF(2)^m$. A bent function has cryptographically ideal nonlinearity, but it is not balanced and is only defined over vector spaces with even dimension. Also $F$ is bent if and only if $b \cdot F$ is bent for any $b \in GF(2)^n$. The following Lemma follows immediately from the definition of bent function [1,2] and Lemma 2.14 in [4].

**Lemma 6.** Let $F$ be a bent function. Then for any vector $b$ in $GF(2)^n$ we have the followings:

1. $b \cdot F$ satisfies PC of degree $k$ for all $1 \leq k \leq n$.
2. $b \cdot F$ satisfies SAC.
3. $b \cdot F$ has maximum nonlinearity.
4. $b \cdot F$ has no linear structure.
5. $b \cdot F$ is not balanced.

We define the Auto-correlation $\Delta_F(a)$ of $F$ with a shift $a$ as follows.

**Definition 1.** Let $F$ be a vector Boolean function on $GF(2)^n$ to $GF(2)^m$. For any vector $a \in GF(2)^n$ the auto-correlation of $F$ with a shift $a$ is defined as

$$\Delta_F(a) = \left( \frac{1}{2^m - 1} \sum_{b \neq 0} \Delta^2_{b,F}(a) \right) ^{\frac{1}{2}}.$$

By definition if $\Delta_F(a) = 0$, $b \cdot F$ satisfies Propagation Characteristic for all $b \in GF(2)^n$ and $a$. The converse is also true. Now we want to derive upper bounds and a lower bound on linearity of vector Boolean functions.
Theorem 1. For any function $F$ on $GF(2)^n$, the nonlinearity of $F$ satisfies

$$N_f \leq 2^{n-1} - \frac{1}{2} \sqrt{2^n + \sum_{j=1}^{2^n-1} \Delta_F^2(a_j)}.$$ 

Proof. Firstly, for $b^*$ in $GF(2)^{m^*}$ we may assume the following equality holds.

$$\sum_{j=1}^{2^n-1} \Delta_F^2(a_j) = \max \left\{ \sum_{j=1}^{2^n-1} \Delta_{b^*F}(a_j) \right\}.$$ 

The right hand side of the inequality of Theorem 3.2 is

$$2^{n-1} - \frac{1}{2} \sqrt{2^n + \sum_{j=1}^{2^n-1} \Delta_F^2(a_j)}$$

$$= 2^{n-1} - \frac{1}{2} \sqrt{2^n + \sum_{j=1}^{2^n-1} 1} \sum_{j=1}^{2^n-1} \Delta_{b^*F}(a_j)$$

$$\geq 2^{n-1} - \frac{1}{2} \sqrt{2^n + \sum_{b \neq 0}^{2^{m-1}} 1} \sum_{j=1}^{2^n-1} \Delta_{b^*F}(a_j)$$

$$= 2^{n-1} - \frac{1}{2} \sqrt{2^n + \sum_{j=1}^{2^n-1} \Delta_{b^*F}^2(a_j)} \quad (by \ definition \ of \ b^*)$$

$$\geq N_{b^*F} \quad (by \ Lemma \ 2.3.)$$

$$\geq N_F. \quad (by \ definition \ of \ N(F))$$

□

Theorem 2. For any function $F$ on $GF(2)^n$, the nonlinearity of $F$ satisfies

$$N_F \leq 2^{n-1} - \frac{1}{2} \sqrt{2^n + \Delta_F^\text{max}}$$

where, $\Delta_F^\text{max} = \max \{ \Delta_F(a) | a \in GF(2)^{n^*} \}.$

Proof. For $a^* \in GF(2)^{n^*}$ and $b^* \in GF(2)^{m^*}$ we may assume the following equality holds.

$$\Delta_F^{a^*} = \Delta_F^\text{max} \quad and \quad \Delta_{b^*F}^2(a^*) = \max \{ \Delta_{b^*F}^2(a) | b^* \in GF(2)^{m^*} \}.$$ 

The right hand side of the inequality of Theorem 3.4 is
\[ 2^{n-1} - \frac{1}{2} \sqrt{2^n + \Delta_{\text{max}} F} \]
\[ = 2^{n-1} - \frac{1}{2} \sqrt{2^n + \Delta_F (a^*)} \quad \text{(by definition of } a^*) \]
\[ = 2^{n-1} - \frac{1}{2} \sqrt{2^n + \left( \frac{1}{2^m - 1} \sum_{b \neq 0} \Delta_{b,F}^2 (a^*) \right)} \]
\[ = 2^{n-1} - \frac{1}{2} \sqrt{2^n + \left( \frac{1}{2^m - 1} \sum_{b \neq 0} \Delta_{b,F}^2 (a^*) \right)} \quad \text{(by definition of } b^*) \]
\[ = 2^{n-1} - \frac{1}{2} \sqrt{2^n + \Delta_{b^*,F} (a^*)} \]
\[ = 2^{n-1} - \frac{1}{2} \sqrt{2^n + \Delta_{\text{max}} F} \quad \text{(by definition of } \Delta_{\text{max}} F) \]
\[ \geq N_{b,F} \quad \text{(by Lemma 3.3.)} \]
\[ \geq N_F. \quad \text{(by definition of } N(F)) \]

\[ \square \]

**Theorem 3.** For any function \( F \) on \( GF(2)^n \), the nonlinearity of \( F \) satisfies

\[ N_f \geq 2^{n-2} - \frac{1}{4} \Delta_{\text{min}}^\text{F} \]

where \( \Delta_{\text{min}}^\text{F} = \max \{ \Delta_{b,F}^\text{min} | b \in GF(2)^m \} \).

**Proof.** It follows immediately from the definition \( \Delta_{\text{min}}^\text{F} \).

\[ \square \]

### 4. Global avalanche characteristics of vector Boolean functions

In this section we want to introduce two indicators to measure the overall avalanche characteristics of vector Boolean functions. The overall avalanche characteristic of a function \( f \) can be measured by examining \( |\Delta(a)| \) for all nonzero vectors \( a \). We can say that a function has a good GAC(Global Avalanche Characteristic) if for most nonzero \( a \), \( |\Delta(a)| \) is zero or very close to zero. This observation leads us to the following definition [5,7,8]. Let \( F : GF(2)^n \rightarrow GF(2)^m \).
be a vector Boolean function. We define the sum-of-square indicator $\sigma_F$ for the Global avalanche characteristics of $F$ by

$$\sigma_F = \sum \Delta^2_F(a) = \sum_a \frac{1}{2^m - 1} \sum_{b \neq 0} \Delta^2_{b,F}(a)$$

and the absolute indicator $\Delta_F$ for the Global avalanche characteristic of $F$ by

$$\Delta_F = \max\{\Delta_F(a) | a \in GF(2)^n\}.$$ 

The smaller $\sigma_F$ and $\Delta_F$ the better the GAC of a function $F$. Also in general the larger the nonlinearity the smaller (i.e. the better) the GAC of a function $F$. 

**Proposition 1.** Let $F : GF(2)^n \rightarrow GF^m$ be a vector Boolean function on $GF(2)^n$. Then we have

1. $2^{2n} \leq \sigma_F \leq 2^{3n}$
2. $\sigma_F = 2^{2n}$ if and only if $F$ is a bent function.
3. $\sigma_F = 2^{3n}$ if and only if $F$ is an affine function.

**Proof.** It follows immediately from definition $\sigma_F$ of and Theorem 3.2 in [4]. □

We also define the sum-of-square indicator $R_{\sigma_F}$ of $F$ and the absolute indicator $R_{\Delta_F}$ of $F$ as follows:

$$R_{\sigma_F} = \frac{\sigma_F - 2^{2n}}{2^{3n} - 2^{2n}}, R_{\Delta_F} = \frac{\Delta_F}{2^n}$$

**Proposition 2.** Let $F : GF(2)^n \rightarrow GF(2)^m$ be a vector Boolean function on $GF(2)^n$. Then

1. $0 \leq R_{\sigma_F} \leq 1, 0 \leq R_{\Delta_F} \leq 1$
2. $R_{\sigma_F} = 0$ if and only if $R_{\Delta_F} = 0$ if and only if $F$ is a bent function.
3. $R_{\sigma_F} = 1$ if and only if $R_{\Delta_F} = 1$ if and only if $F$ is an affine function.

**Proof.** It follows immediately from definition of $R_{\sigma_F}$ and $R_{\sigma_F}$. □

**Discussions and examples**

Here we present the nonlinearities, the values of the sum-of-square indicator and the absolute indicator for the S-boxes of DES and Rijndael. Firstly, the description of S-boxes of DES is given in [4]. We have the following nonlinearity and indicator values for $S_i$-boxes $i = 1, 2, \cdots, 8$ of DES.
In case of DES, among $S_i$-boxes, $1 \leq i \leq 8$, $S_4$-box has the highest nonlinearity. As far as a global avalanche characteristic concerns all $S_i$-boxes $1 \leq i \leq 8$ behave pretty evenly.

The description of $S$-box of Rijndael is given in [3]. We have the following nonlinearity and indicator values for $S$-box of Rijndael.

\begin{table}
\centering
\begin{tabular}{|c|c|c|c|c|}
\hline
 & $N_F$ & $\sigma_F$ & $R_{\sigma_F}$ & $\Delta_F$ & $R_{\Delta_F}$ \\
\hline
$S_1$ & 24 & 19032 & 0.058 & 48 & 0.750 \\
$S_2$ & 24 & 19512 & 0.060 & 48 & 0.750 \\
$S_3$ & 24 & 19912 & 0.061 & 40 & 0.625 \\
$S_4$ & 26 & 18792 & 0.057 & 48 & 0.750 \\
$S_5$ & 24 & 19992 & 0.062 & 48 & 0.750 \\
$S_6$ & 24 & 19704 & 0.060 & 48 & 0.750 \\
$S_7$ & 24 & 20064 & 0.060 & 48 & 0.750 \\
$S_8$ & 24 & 18720 & 0.057 & 40 & 0.625 \\
\hline
\end{tabular}
\caption{Table 4.1}
\end{table}

The $S$-box of Rijndael was generated using $x^{-1}$, i.e. $x^{255}$ so that a bijection function $x^n$, $0 \leq n \leq 255$ have the best differential property and linear approximation. Here we consider the $S$-box

$$S(x) = Ax^n + B$$

for $n = 1, 2, \ldots, 255$ and calculate the corresponding indicator values which are given in table 5.4. From table 5.4 we can see the smallest the sum-of-square indicator value is 423108 and this value is yielded when exponent $n$’s are 127, 191, 223, 239, 247, 251, 253, 254 and 255.

\begin{table}
\centering
\begin{tabular}{|c|c|c|c|c|}
\hline
 & $N_F$ & $\sigma_F$ & $R_{\sigma_F}$ & $\Delta_F$ & $R_{\Delta_F}$ \\
\hline
$S$ & 112 & 423108 & 0.0213 & 136 & 0.53125 \\
\hline
\end{tabular}
\caption{Table 4.2}
\end{table}

References


Wansoon Kim received her MS from Sogang University and Ph.D at Indiana University (Bloomington, USA). Since 1989 she has been a professor at Hoseo University. Her research interests focus on Infinite dimensional Lie Algebras, Applied Algebras and Cryptography.

Department of Mathematics, Hoseo University, Asansi, Chungnam 337-850, Korea
e-mail: kimws@office.hoseo.ac.kr

Hee-Sung Hwang received his BS in 2002 and MS from Hoseo University in 2004. His research interests focus on Applied Algebras and Cryptography.

Department of Mathematics, Hoseo University, Asansi, Chungnam 337-850, Korea
e-mail: hshwang@office.hoseo.ac.kr