The algebraic immunity of a class of correlation immune H Boolean functions

Jinglian Huang^a and Zhuo Wang

School of Electrical Engineering, Northwest University for Nationalities, Lanzhou, China

Abstract. Using the derivative of the Boolean function and the e-derivative defined by ourselves as research tools, we study the algebraic immunity of a class of H Boolean functions, getting solutions to solve annihilators of the lowest algebraic degree of H Boolean functions by formulas, the existence and solution of the 1st-order algebraic immunity functions. Meanwhile we obtain that when H Boolean functions are 1st-order algebraic immunity functions, the relationship between 1st-degree annihilator and e-derivative, the solving formula of 1st-degree annihilator represented by the derivative and the e-derivative, and the compatibility of the 1st-order algebraic immunity and the higher-order correlation immunity of H Boolean functions.

Keywords: H Boolean functions; e-derivative; algebraic immunity; correlation immunity; annihilators.

1 Introduction

The cipher security is the core of the cryptosystem, and only a cryptosystem with good security has an existing significance. Boolean functions with a variety of secure cipher properties are the key factors to design the cryptosystem with the ability to resist multiple cipher attacks and good safety performance. It is of great importance for a security cryptosystem to study some properties of Boolean functions, which make the cryptosystem resist various attacks [1], such as high algebraic degree, high nonlinearity, the strict avalanche criterion and propagation, higher-order correlation immunity and higher-order algebraic immunity. Therefore, there are some important research problems, such as the existence, the feature, the design, the construction and the count of Boolean functions with some kind of secure cryptographic property. Among them, the algebraic immunity of Boolean functions is current central issues [2~6].

The H Boolean functions have the propagation property. When we study the correlation immunity and algebraic immunity of the H Boolean functions, it is equivalent to study the compatibility of the propagation property, algebraic immunity and correlation immunity of Boolean functions. It is the basis of studying the correlation immunity and algebraic immunity of the H Boolean functions to study the correlation immunity and algebraic immunity of the H Boolean functions with the Hamming weight of $2^{n-1} + 2^{n-2}$. In this paper, using the derivative and e-derivative [7~9] as research tools, we study the importance of study cryptographic properties of H Boolean function with Hamming weight of $2^{n-1} + 2^{n-2}$.

^a Corresponding author : huangjlwork@163.com

2 Preliminaries

To study cryptographic properties of H Boolean functions, we proposed the concept of the e-derivative. The e-derivative and derivative are defined here as Definition 1&2.

Definition 1: The e-derivative (e-partial derivative) of n -dimensional Boolean functions $f(x) = f(x_1, x_2, \dots, x_n) \in GF(2)^{GF(2)^n}$ for r variables $x_{i_1}, x_{i_2}, \dots, x_{i_r}$ ($i, r \in [1, n]$) is defined as

$$\begin{aligned} & ef(x)/e(x_{i_1}, x_{i_2}, \dots, x_{i_r}) \\ &= f(x_1, x_2, \dots, x_{i_1}, x_{i_2}, \dots, x_{i_r}, \dots, x_n) f(x_1, x_2, \dots, 1+x_{i_1}, 1+x_{i_2}, \dots, 1+x_{i_r}, \dots, x_n). \end{aligned} \quad (1)$$

If $r = 1$, (1) turns into the e-derivative of $f(x) = f(x_1, x_2, \dots, x_n)$ for a single variable, which is denoted by $ef(x)/ex_i$ ($i = 1, 2, \dots, n$). As a result, the simplified form below can be easily derived.

$$ef(x)/ex_i = f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) \quad (i = 1, 2, \dots, n).$$

Definition 2: The derivative (partial derivative) of n -dimensional Boolean functions $f(x) = f(x_1, x_2, \dots, x_n) \in GF(2)^{GF(2)^n}$ for r variables $x_{i_1}, x_{i_2}, \dots, x_{i_r}$ ($i, r \in [1, n]$) is defined as

$$\begin{aligned} & \partial f(x)/\partial(x_{i_1}, x_{i_2}, \dots, x_{i_r}) \\ &= f(x_1, x_2, \dots, x_{i_1}, x_{i_2}, \dots, x_{i_r}, \dots, x_n) + f(x_1, x_2, \dots, 1+x_{i_1}, 1+x_{i_2}, \dots, 1+x_{i_r}, \dots, x_n). \end{aligned} \quad (2)$$

If $r = 1$, (2) turns into the derivative of $f(x) = f(x_1, x_2, \dots, x_n)$ for a single variable, which is denoted by $df(x)/dx_i$ ($i = 1, 2, \dots, n$). As a result, the simplified form below can be easily derived.

$$d f(x)/d x_i = f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) + f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) \quad (i = 1, 2, \dots, n).$$

According to Definition 1&2, we can get Lemmas 1&2 easily.

Lemma 1: A Boolean function is a function with propagation of degree r iff

$$w_i(\partial f(x)/\partial(x_{i_1}, x_{i_2}, \dots, x_{i_r})) = 2^{n-1} \quad (1 \leq i \leq n, 1 \leq r \leq n, 1 \leq i_1 \leq i_2 \leq \dots \leq i_r \leq n).$$

A Boolean function $f(x)$ is an H Boolean function iff the following equations hold for all x_i :

$$w_i(df(x)/dx_i) = 2^{n-1} \quad (i = 1, 2, \dots, n). \quad (3)$$

Lemma 2: For any arbitrary Boolean function $f(x)$, the following equations are true:

$$f(x) = f(x)df(x)/dx_i + ef(x)/ex_i \quad (i = 1, 2, \dots, n), \quad (4)$$

and

$$\begin{aligned} w_i(f(x)) &= w_i(f(x)df(x)/dx_i) + w_i(ef(x)/ex_i) \\ &= 2^{-1}w_i(df(x)/dx_i) + w_i(ef(x)/ex_i) \end{aligned} \quad (i = 1, 2, \dots, n). \quad (5)$$

3 The algebraic immunity of a class of correlation immune H Boolean functions

We discuss the cryptographic properties of H Boolean functions $f(x)$ with the Hamming weight of $2^{n-1} + 2^{n-2}$ (There is $w_i(f(x)) = 2^{n-2}$ correspondingly), such as algebraic immunity, annihilators, algebraic immunity functions and correlation immunity.

In Theorem 1, when the H Boolean function $f(x)$ with the Hamming weight of $2^{n-1} + 2^{n-2}$ is the sum of two sub-Boolean functions $g(x)$ and $h(x)$, and $g(x)$ is a linear function, we will discuss the relationship between $g(x)$ and $e f(x)/ex_n$, the relationship between $g(x)$ and the annihilator of the lowest algebraic degree, the algebraic degree of $f(x)$, the lower bound of the correlation immunity order of $f(x)$, the algebraic immunity order of $f(x)$ and so on.

Theorem 1: For H Boolean functions $f(x)$ with $w_t(f(x)) = 2^{n-1} + 2^{n-2}$, suppose $g(x)$ and $h(x)$ are sub-functions of H Boolean functions $f(x)$, and get $f(x) = g(x) + h(x)$ and $g(x)h(x) = 0$. If $g(x)$ is a linear function (or affine function), then

- 1) For all $i = 1, 2, \dots, n$, we have $w_t(dh(x)/dx_i) = 2^{n-1}$.
- 2) $g(x)$ doesn't contain x_n term, iff $g(x) = ef(x)/ex_n$. When $g(x)$ doesn't contain x_n term, there must have $h(x) = f(x)df(x)/dx_n$.
- 3) When $g(x)$ contains x_n term, there must have $h(x) = (1 + g(x))ef(x)/ex_n$.
- 4) The algebraic degree $\deg f(x) = 2$.
- 5) The correlation immune order $CI(f(x)) \geq 1$, $g(x)$ is an annihilator of the lowest algebraic degree of $f(x)$, and the algebraic immunity order $AI(f(x)) = 1$.

Proof: 1) Since g is a linear function, for all $i = 1, 2, \dots, n$, there is

$$\frac{dg(x)}{dx_i} = \begin{cases} 1, & (\text{when } g(x) \text{ contain } x_i \text{ item}) \\ 0, & (\text{when } g(x) \text{ doesn't item contain } x_i \text{ item}) \end{cases} \quad (6)$$

By the known conditions of $f(x)$ and Lemma 1, we can get

$$\begin{cases} w_t(f(x)) = 2^{n-1} + 2^{n-2}, & w_t(df(x)/dx_i) = 2^{n-1} \\ f(x) = g(x) + h(x), & g(x)h(x) = 0 \end{cases} \quad (i = 1, 2, \dots, n).$$

So we deduce

$$\begin{aligned} & w_t(df(x)/dx_i) \\ &= w_t(dg(x)/dx_i) + w_t(dh(x)/dx_i) - 2w_t(dg(x)/dx_i dh(x)/dx_i) = 2^{n-1} \quad (i = 1, 2, \dots, n). \end{aligned} \quad (7)$$

By (6) and (7), for all $i = 1, 2, \dots, n$, there is $w_t(dh(x)/dx_i) = 2^{n-1}$ ($i = 1, 2, \dots, n$).

2) If $g(x) = ef(x)/ex_n$, $g(x)$ doesn't contain x_n term obviously. Then we have $f(x) = f(x)df(x)/dx_n + ef(x)/ex_n = f(x)df(x)/dx_n + g(x) = h(x) + g(x)$.

So we can know $h(x) = f(x)df(x)/dx_n$. Conversely, if $g(x)$ doesn't contain x_n term, it means $f(x)$ contains linear sub-functions because of $g(x)f(x) = g(x)$. And because of

$$\begin{cases} w_t(f(x)) = 2^{n-1} + 2^{n-2}, & w_t(f(x)df(x)/dx_n) = 2^{n-2} \\ w_t(ef(x)/ex_n) = 2^{n-1}, & w_t(df(x)/dx_n) = 2^{n-1} \end{cases},$$

we can know that there must be $\deg(ef(x)/ex_n) = 1$. Namely, $ef(x)/ex_n$ which doesn't contain x_n term is a linear function. Because the Hamming weight of the linear function $g_i(x)$ is 2^{n-1} , and $g_i(x)$ are solutions of the equation $g_i(x)f(x) = g_i(x)(f(x)df(x)/dx_n + ef(x)/ex_n) = g_i(x)$. Then we can know that there exist only another two linear sub-functions $g_1(x)$ and $g_2(x)$, which satisfy

$$g_i(x) = f(x)df(x)/dx_n + f_i(x) \quad (i=1,2). \quad (8)$$

For (8), $f_i(x) = f_i(x)ef(x)/ex_n$ ($i=1,2$) and $w_i(f_i(x)) = 2^{-1}w_i(ef(x)/ex_n) = 2^{n-2}$ ($i=1,2$). That is to say, $f_i(x)$ ($i=1,2$) is sub-function of $ef(x)/ex_n$, and its Hamming weight is half of $ef(x)/ex_n$'s. So

$$\begin{aligned} df_i(x)/dx_n &= d(f_i(x)ef(x)/ex_n)/dx_n \\ &= df_i(x)/dx_n ef(x)/ex_n + f_i(x)d(ef(x)/ex_n)/dx_n + df_i(x)/dx_n d(ef(x)/ex_n)/dx_n \quad (i=1,2). \\ &= df_i(x)/dx_n ef(x)/ex_n = ef(x)/ex_n \end{aligned}$$

Then

$$\begin{aligned} dg_i(x)/dx_n &= d(f(x)df(x)/dx_n)/dx_n + df_i(x)/dx_n \\ &= df(x)/dx_n + f(x)d(df(x)/dx_n)/dx_n + df(x)/dx_n d(df(x)/dx_n)/dx_n + df_i(x)/dx_n \quad (i=1,2). \\ &= df(x)/dx_n + 0 + 0 + ef(x)/ex_n = 1 \neq 0 \end{aligned}$$

We can know, $g_i(x)$ is a linear function which contains x_n term.

Because $f(x)$ has if and only if three linear sub-functions: one linear sub-function is $ef(x)/ex_n$ which doesn't contain x_n term, and two linear sub-functions are $g_i(x) = f(x)df(x)/dx_n + f_i(x)$ ($i=1,2$) which contain x_n term, we can know $g(x) = ef(x)/ex_n$ and $h(x) = f(x)df(x)/dx_n$.

3) When $g(x)$ contains x_n term, namely $g(x) = f(x)df(x)/dx_n + f_i(x)$ ($i=1,2$). Let $h(x) = ef(x)/ex_n + f_i(x)$ ($i=1,2$), we have

$$\begin{aligned} (1 + g(x))ef(x)/ex_n \\ = ef(x)/ex_n + f(x)df(x)/dx_n ef(x)/ex_n + f_i(x)ef(x)/ex_n = ef(x)/ex_n + f_i(x) = h(x). \end{aligned}$$

Hence when $g(x)$ contains x_n term, namely $g(x) = f(x)df(x)/dx_n + f_i(x)$ ($i=1,2$) (which $f_i(x) = f_i(x)ef(x)/ex_n$), there is $h(x) = (1 + g(x))ef(x)/ex_n$.

4) As $ef(x)/ex_n$ is a linear function, and $df(x)/dx_n + ef(x)/ex_n = 1$. Then $df(x)/dx_n$ is a linear function too.

Due to $w_i(f(x)) = 2^{n-1} + 2^{n-2}$ and $w_i(df(x)/dx_i) = 2^{n-1}$ ($i=1,2,\dots,n$), linear function $ef(x)/ex_n$ can only be

$$ef(x)/ex_n = \sum_{i=1}^{n-1} x_i \quad \text{or} \quad ef(x)/ex_n = \sum_{i=1}^{n-2} x_i. \quad (9)$$

So when $i=1,2,\dots,n-1$, we have

$$ef(x)/ex_i = \sum_{i=1}^{n-2} x_i + x_n \quad \text{or} \quad ef(x)/ex_i = 1 + x_n + \sum_{i=1}^{n-2} x_i \quad \text{or} \quad ef(x)/ex_i = x_{n-1} + x_n.$$

Therefore, for all $i=1,2,\dots,n$, there is

$$\deg(df(x)/dx_i) = \deg(1 + ef(x)/ex_i) = 1. \quad (10)$$

As $f(x)d f(x)/d x = f(x) + ef(x)/ex_n$, there is

$$\begin{aligned} d(f(x)df(x)/dx_n)/dx_i &= df(x)/dx_i + d(ef(x)/ex_n)/dx_i \\ &= df(x)/dx_i + d(1 + df(x)/dx_n)/dx_i = df(x)/dx_i + d(df(x)/dx_n)/dx_i \quad (i=1,2,\dots,n). \end{aligned} \quad (11)$$

Because of $\deg(df(x)/dx_i) > \deg(d(df(x)/dx_n)/dx_i)$ ($i = 1, 2, \dots, n$), known from (11) and (10),

$$\deg(d(f(x)df(x)/dx_n)/dx_i) = \deg(df(x)/dx_i) = 1 \quad (i = 1, 2, \dots, n). \quad (12)$$

So we get

$$\deg(f(x)df(x)/dx_n) = 2. \quad (13)$$

Known by (6), therefore $\deg f(x) = \deg(f(x)d f(x)/dx_n) = 2$.

5) By (9), we can know, for all $i = 1, 2, \dots, n$, there is $w_i(x_i ef(x)/ex_n) = 2^{n-2}$. Since

$$\begin{cases} w_i(f(x)) = 2^{n-1} + 2^{n-2}, & w_i(df(x)/dx_i) = 2^{n-1} \\ df(x)/dx_n + ef(x)/ex_n = 1, & w_i(ef(x)/ex_n) = 2^{n-1} \end{cases} \quad (i = 1, 2, \dots, n),$$

we can know, there are $\partial f(x)/\partial(x_{n-2}x_{n-1}x_n) = 0$ or $\partial f(x)/\partial(x_{n-1}x_n) = 0$. So

$$w_i(x_i f(x)df(x)/dx_n) = 2^{n-3} \quad (i = 1, 2, \dots, n).$$

For the kind of functions like $ef(x)/ex_n = \sum_{i=1}^{n-1} x_i$, there also be

$$w_i((x_i + x_j)ef(x)/ex_n) = 2^{n-2}, \text{ and } w_i((x_i + x_j)f(x)df(x)/dx_n) = 2^{n-3} \quad (i, j = 1, 2, \dots, n, i \neq j).$$

But for the kinds of functions like $ef(x)/ex_i = \sum_{i=1}^{n-2} x_i$ and $ef(x)/ex_i = x_{n-1} + x_n$ ($i = 1, 2, \dots, n-1$),

we have $w_i((x_{n-1} + x_n)f(x)df(x)/dx_n) = 2^{n-2} > 2^{n-3}$.

Because $w_i(f(x) + \omega x) = w_i(f(x)df(x)/dx_n + \omega x) + w_i(ef(x)/ex_n + \omega x) - w_i(\omega x)$, we have $CI(f(x)) \geq 1$.

By the known conditions $f(x) = g(x) + h(x)$ and $g(x)h(x) = 0$, we can get $g(x)f(x) = g(x)$. So $g(x)(1 + f(x)) = 0$, i.e. $g(x)$ are annihilators of $1 + f(x)$.

By the known condition: $g(x)$ is a linear function, and the sub-function of $1 + f(x)$ is an annihilator of $f(x)$ (i.e. $f(x)$ have nonzero annihilators), we can get that, $g(x)$ is an annihilator of the lowest algebraic degree of $f(x)$ and $1 + f(x)$, there is $AI(f(x)) = 1$.

The proof ends.

From (8) in the proof of Theorem 1, we can know, in (8), $f_i(x)$ should have exact expressions as Corollary 1.

Corollary 1: For linear annihilators $f(x)df(x)/dx_n + f_i(x)$ of $1 + f(x)$ in Theorem 1, the concrete expressions of $f_i(x)$ are $f_i(x) = f(x)df(x)/dx_n + ef(x)/ex_{n-1}ef(x)/ex_n$, and

$$f_i(x) = f(x)df(x)/dx_n + ef(x)/e(x_{n-1}x_n)ef(x)/ex_n.$$

Corollary 2: $1 + f(x)$ have linear annihilators $ef(x)/ex_n$ in Theorem 1.

Following we will further discuss the existence theorem of H Boolean Functions, which correlation immunity order is the highest and algebraic immunity is 1-order.

The problem is not been solved explicitly and not been proved all the time, which when the constant Boolean functions have $n-1$ or n order correlation immune, the highest order of the non-const Boolean functions can reach $n-2$. In the theorem 2, we get the result that there exist non-zero the H Boolean functions with the highest order correlation immune ($n-2$) and the 1-order algebraic immunity.

Theorem 2: For H Boolean functions with $w_t(f(x)) = 2^{n-1} + 2^{n-2}$, there exists the kind of H Boolean Functions with the algebraic immunity order $AI(f) = 1$ and the correlation immunity order $CI(f) = n - 2$.

Proof: As $w_t(f(x)) = 2^{n-1} + 2^{n-2}$, and $f(x)$ are H Boolean Functions, there are

$$w_t(f(x)df(x)/dx_n) = 2^{n-2}, \text{ and } w_t(df(x)/dx_n) = w_t(ef(x)/ex_n) = 2^{n-1}.$$

So there is

$$df(x)/dx_n + ef(x)/ex_n = 1. \quad (14)$$

Therefore, $f(x)$ must satisfy: a) When $n - i$ is odd, we have

$$w_t(\partial f(x)/\partial(x_i, x_{i+1}, \dots, x_{n-1}, x_n)) = 2^{n-1}; \quad (15)$$

b) When $n - i$ is even, there is

$$w_t(\partial f(x)/\partial(x_i, x_{i+1}, \dots, x_{n-1}, x_n)) = 0 \quad \text{or} \quad w_t(\partial f(x)/\partial(x_i, x_{i+1}, \dots, x_{n-1}, x_n)) = 2^{n-1}. \quad (16)$$

Let $g(x) = \sum_{i=1}^{n-1} x_i$, when $n - i$ is odd, we have

$$w_t(\partial g(x)/\partial(x_i, x_{i+1}, \dots, x_{n-1}, x_n)) = 1; \quad (17)$$

When $n - i$ is even, we have

$$w_t(\partial g(x)/\partial(x_i, x_{i+1}, \dots, x_{n-1}, x_n)) = 0. \quad (18)$$

Compared with (17) and (15), (18) and (16), we can take $ef(x)/ex_n = g(x)$ and $df(x)/dx_n = 1 + g(x)$.

The two expressions in (16) are different because the values of $f(x)df(x)/dx_n$ are different (but the values of $ef(x)/ex_n$ are the same). So we can know, there exists H Boolean Functions with $w_t(f(x)) = 2^{n-1} + 2^{n-2}$ and there is

$$ef(x)/ex_n = \sum_{i=1}^{n-1} x_i = g. \quad (19)$$

Obviously, $g(1 + f(x)) = 0$. Hence we can know, $AI(f(x)) = 1$.

Since $f(x)$ satisfy (19), for all ωx and $1 \leq w_t(\omega) \leq n - 2$, there is

$$w_t(\omega x ef(x)/ex_n) = w_t(\omega x \sum_{i=1}^{n-1} x_i) = 2^{n-2}. \quad (20)$$

From (14) and (20), we can know $w_t(\omega x df(x)/dx_n) = 2^{n-2}$.

The same with the proof of (11), (12) and (13) in Theorem 1, there is

$$w_t(\omega x f(x)df(x)/dx_n) = 2^{n-3}. \quad (21)$$

By (20),(21) and the following

$$w_i(f(x) + \omega x) = w_i(f(x)df(x)/dx_n + \omega x) + w_i(ef(x)/ex_n + \omega x) - w_i(\omega x),$$

we can know, there must be $CI(f(x)) = n - 2$.

The proof ends.

Corollary 3: In Theorem 2, $1 + f(x)$ have linear annihilators $g(x)$, and $g(x) = ef(x)/ex_n$.

Example 1: There is an H Boolean function $f(x)$ with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$ and $n = 4$, $f(x) = 1 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4$.

There are $\deg f(x) = 2$, $ef(x)/ex_4 = x_1 + x_2 + x_3$, and

$$f(x)df(x)/dx_4 = 1 + x_1 + x_2 + x_3 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4.$$

$f(x)$ is a 2-order($n - 2 = 4 - 2 = 2$) correlation immune function.

$f(x)$ and $1 + f(x)$ have annihilators of the lowest algebraic degree $g(x) = x_1 + x_2 + x_3$. So $AI(f(x)) = 1$, i.e. $f(x)$ is an H Boolean function with $AI(f(x)) = 1$ and $CI(f(x)) = n - 2$.

Theorems 1&2 respectively prove the existence of 1-order algebraic immunity of H Boolean functions with correlation immunity of order 1 and $n - 2$, and $ef(x)/ex_n$ is an annihilator of the lowest algebraic degree of H Boolean function. But when H Boolean functions meet $w_i(f(x)) = 2^{n-1} + 2^{n-2}$, there should exists a lot of H Boolean functions that the algebraic degree of $ef(x)/ex_n$ is not less than 1. Therefore, the existence of these H Boolean functions is need to be studied, and when such functions exist, the maximum of its algebraic immunity should also be noticed. It comes to Theorem 3.

In Theorem 3, the existence of H Boolean functions $f(x)$ with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$, whose algebraic immunity and algebraic degree are not less than 2, will be discussed.

Theorem 3: For H Boolean function with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$, if $\deg(ef(x)/ex_n) > 1$, we have : 1) $\deg f(x) > \deg(ef(x)/ex_n)$; 2) $AI(f(x)) \geq 2$.

Proof: 1) $f(x)$ is an H Boolean function with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$, so $\begin{cases} w_i(df(x)/dx_i) = 2^{n-1} \\ w_i(ef(x)/ex_i) = 2^{n-1} \end{cases}$.

Therefore

$$df(x)/dx_n = 1 + ef(x)/ex_n. \quad (22)$$

By Lemma 2, we can know,

$$f(x) = f(x)df(x)/dx_n + ef(x)/ex_n. \quad (23)$$

Since

$$d(f(x)df(x)/dx_n)/dx_n = df(x)/dx_n, \quad (24)$$

by (22) and (24), we have

$$\deg(f(x)df(x)/dx_n) > \deg(df(x)/dx_n) = \deg(ef(x)/ex_n). \quad (25)$$

Known By (23) and (25), there exists an H Boolean function $f(x)$ which satisfies $\deg(ef(x)/ex_n) > 1$ and

$$\deg f(x) = \deg(f(x)df(x)/dx_n) > \deg(ef(x)/ex_n). \quad (26)$$

2) From the proof of Theorem 1&2, we can know that if $f(x)$ have 1-st subfunctions, they would only be $ef(x)/ex_n$ and $g(x) = f(x)df(x)/dx_n + f_i(x)$ ($i=1,2$) (in which $f_i(x) = f_i(x)ef(x)/ex_n$ and $w_i(f_i(x)) = 2^{n-2}$). In H Boolean function with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$, there exists functions which satisfy $\deg(ef(x)/ex_n) > 1$. Therefore, if $\deg(ef(x)/ex_n) > 1$, 1-st subfunctions don't exist. As $w_i(1+f(x)) = 2^{n-2}$, both $1+f(x)$ and $f(x)$ don't have 1-st annihilators, so $AI(f(x)) \geq 2$.

This completes the proof.

Corollary 4: For H Boolean function $f(x)$ with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$, if $AI(f(x)) \geq 2$, there must be $\deg(ef(x)/ex_n) > 1$.

Remark: The result of Theorem 3 is only true for the H Boolean functions with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$. Thanks to the existence of (22), we can get (25) and (26). For other kinds of H Boolean functions, the result of Theorem 3 can't always be correct.

Example 2: There is a 4-variable rotation symmetric H Boolean function $f(x)$,

$$f(x) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4.$$

There are $w_i(f(x)) = 2^{n-1} + 2^{n-3} < 2^{n-1} + 2^{n-2}$ and $\deg f(x) = 2$, but

$$ef(x)/ex_4 = x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3,$$

and

$$f(x)df(x)/dx_4 = x_1x_4 + x_2x_4 + x_3x_4 + x_1x_2x_3.$$

We have $\deg(ef(x)/ex_4) = \deg(f(x)df(x)/dx_4) = 3$.

$f(x)$ and $1+f(x)$ have annihilators of the lowest algebraic degree $g(x) = x_1x_2 + x_3x_4$, i.e.

$AI(f(x)) = 2 = \left\lfloor \frac{4}{2} \right\rfloor$. $f(x)$ also is an optimal algebraic immunity function, but it not a correlation immune function.

For H Boolean functions with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$, there exist functions with algebraic immunity order $AI(f) = 1$ and correlation immune order $CI(f(x)) = 1$. And the derivative and e-derivative of this kind of H Boolean functions have their own characteristics. Since this kind of functions is easy to be structured and proved. Theorem 4 is given here without the proof.

Theorem 4: For H Boolean functions $f(x)$ with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$, if having

$$\begin{cases} w_i(ef(x)/e(x_{n-1}x_n)) = 2^{n-1} + 2^{n-3}, & w_i(\partial f(x)/\partial(x_{n-1}x_n)) = 2^{n-2} \\ w_i(ef(x)/e(x_{n-3}x_{n-2}x_{n-1}x_n)) = 2^{n-1} + 2^{n-3}, & w_i(\partial f(x)/\partial(x_{n-3}x_{n-2}x_{n-1}x_n)) = 2^{n-2} \end{cases},$$

we can get $CI(f(x)) = 1$ and $AI(f(x)) = 1$.

In fact, complementary functions $1+f(x)$ of H Boolean functions $f(x)$ have annihilators

$$x_{n-1} + x_n + \sum_{i=1}^{n-4} x_i \text{ in Theorem 4. And } w_i(f(x) + x_{n-3} + x_{n-2}) = 2^{n-1} + 2^{n-3}, CI(f(x)) = 1.$$

4 Conclusions

The cryptographic properties of Boolean functions are not only connected with the whole values of Boolean functions, but also connected with the values of two different properties and the structure of values. In this paper, using the derivative and e-derivative defined by ourselves, we express the values of two different properties of Boolean functions and discuss the correlation immunity and algebraic immunity of the H Boolean functions with the Hamming weight of $2^{n-1} + 2^{n-2}$. The results show that

we can better solve the annihilator of the lowest algebraic degree Boolean functions using the derivative and the e-derivative.

In the paper, the results are very important. It is very useful to study cryptographic properties of Boolean functions using the derivative and e-derivative.

Acknowledgement

This work is supported by National Natural Science Foundation of China (Grant No. 61262085).

References

1. Q. Wen, X. Niu , Y. Yang. The Boolean Functions in modern cryptology. Beijing: Science Press (2000).
2. Y. Lou, H. Han, C. Tang, et al. Constructing vectorial Boolean functions with high algebraic immunity based on group decomposition. *International Journal of Computer Mathematics*, **65**(4): 1-13, (2015)
3. Y. Chen, Y. Zhang, W. Tian. Construction of Even-variable Rotation Symmetric Boolean Functions with Optimal Algebraic Immunity. *Journal of Cryptologic Research*, **1**(5): 437-448, (2014) (In Chinese)
4. Z. Tu, and Y. Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. *Designs, Codes and Cryptography*, **60**, (1), pp. 1-14, (2011)
5. S. H. Su, X. H. Tang. Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity. *Designs, Codes and Cryptography*, **71**(2): 183-199, (2014)
6. J. Peng, Q. Wu, H. Kan. On symmetric boolean functions with high algebraic immunity on even number of variables. *IEEE Transactions on Information Theory*, **57**, (10), pp. 7205-7220, (2011)
7. J. Huang, Z. Wang. The relationship between correlation immune and weight of H Boolean functions. *Journal on Communications*, **33**(2):110-118(2012). (In Chinese)
8. W. Li, Z. Wang, J. Huang. The e-derivative of boolean functions and its application in the fault detection and cryptographic system. *Kybernetes*, **40**(5-6):905-911(2011).
9. M. Zhao. Method of detecting special logic function based on Boolean e-derivative[J]. *Journal of Zhejiang University (Science Edition)*, **41**(4):424-426, (2014) (In Chinese)