The algebraic immunity and the optimal algebraic immunity functions of a class of correlation immune H Boolean functions

Huang Jinglian[a], and Wang Zhuo

School of Electrical Engineering, Northwest University for Nationalities, Lanzhou, 730030, China

Abstract. We put forward an efficient method to study the algebraic immunity of H Boolean functions with Hamming weight of $2^{n-1}+2^{n-2}$, getting the existence of the higher-order algebraic immunity functions with correlation immunity. We also prove the existing problem of the above 2-order algebraic immunity functions and the optimal algebraic immunity functions. Meanwhile, we solve the compatibility of algebraic immunity and correlation immunity. What is more, the main theoretical results are verified through the examples and are revealed to be correct. Such researches are important in cryptographic primitive designs, and have significance and role in the theory and application range of cryptosystems.

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 $2^{n-1}+2^{n-2}$.

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 $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ for r variables $x_{i1},x_{i2},\cdots,x_{ir}$ is defined as

$$\begin{aligned}&ef(x)/e(x_{i1},x_{i2},\cdots,x_{ir})\\&=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)\cdot\\&f(x_1,x_2,\cdots,1+x_{i1},1+x_{i2},\cdots,1+x_{ir},\cdots,x_n)\\&(1\le i\le n,1\le i_1\le i_2\le\cdots\le i_r\le n,1\le r\le n)\end{aligned}\quad(1)$$

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

$$\begin{aligned}&ef(x)/ex_i\\&=f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)\cdot\ (i=1,2,\cdots,n).\\&f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n)\end{aligned}$$

Definition 2: The derivative (partial derivative) of n-dimensional Boolean functions $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ for r variables $x_{i1},x_{i2},\cdots,x_{ir}$ is defined as

$$\begin{aligned}&\partial f(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir})\\&=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)+\\&f(x_1,x_2,\cdots,1+x_{i1},1+x_{i2},\cdots,1+x_{ir},\cdots,x_n)\\&(1\le i\le n,1\le i_1\le i_2\le\cdots\le i_r\le n,1\le r\le n)\end{aligned}\quad(2)$$

If $r=1$, (2) turns into the derivative of $f(x)=f(x_1,x_2,\cdots,x_n)$ for a single variable, which is

[a] Huang Jinglian: huangjlstudy@163.com

denoted by $df(x)/dx_i$ $(i=1,2,\cdots,n)$. As a result, the simplified form below can be easily derived.

$$\begin{aligned} &df(x)/dx_i \\ &= f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n) \ (i=1,2,\cdots,n). \\ &+f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n) \end{aligned}$$

Definition 3: The cascade function $f(x)$ $(x=x_0x_1x_2\cdots x_n\in GF(2)^{n+1})$ cascade with two n-dimensional Boolean functions $f_1(x')$ and $f_2(x')$ $(x'=x_1x_2\cdots x_n\in GF(2)^n)$ is defined as

$$\begin{aligned} &f(x)=(1+x_0)f_1(x')+x_0f_2(x') \\ &=f_1(x')+x_0(f_1(x')+f_2(x')) \end{aligned},$$

$f(x)$ is denoted by $f(x)=f_1(x)\|f_2(x)$.

According to Definition 1~3, we can get Lemmas 1 easily.

Lemma 1: For any arbitrary Boolean function $f(x)$, the following equations are true:

$$\begin{aligned} &f(x) \\ &=f(x)df(x)/dx_i+ef(x)/ex_i \end{aligned} \quad (i=1,2,\cdots,n), \quad (3)$$

and

$$\begin{aligned} &w_t(f(x)) \\ &=w_t(f(x)df(x)/dx_i)+w_t(ef(x)/ex_i) \\ &=2^{-1}w_t(df(x)/dx_i)+w_t(ef(x)/ex_i) \\ &(i=1,2,\cdots,n) \end{aligned}. \quad (4)$$

3 The algebraic immunity and optimal algebraic immunity functions 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 $w_t(f(x))=2^{n-2}$ correspondingly), such as algebraic immunity, annihilators, optimal algebraic immunity functions and correlation immunity.

In Theorem 1, we discuss the relationship of the algebraic degree of the lowest algebraic degree annihilators among $f_1(x)$, $f_2(x)$ and the cascade function $f(x)$ ($f(x)=f_1(x)\|f_2(x)$). Theorem 1 is a preliminary theorem preparing for Theorem 2.

Theorem 1: If $f(x)=f_1(x)\|f_2(x)$, $g_1(x)$ are annihilators of the lowest algebraic degree of $f_1(x)$ (or $1+f_1(x)$), $g_2(x)$ are annihilators of the lowest algebraic degree of $f_2(x)$ (or $1+f_2(x)$), and $\deg g_1(x)=m_1$, $\deg g_2(x)=m_2$.

1. If $g_1(x)=g_2(x)$ (or $g_1(x)=1+g_2(x)$), $AI(f(x))=m_2=m_1$.

2. If $g_1(x)\neq g_2(x)$ and $g_1(x)\neq 1+g_2(x)$,

1) If $m_1\geq m_2+1$ and $g_2(x)f_1(x)\neq 0$, $AI(f(x))=m_2+1$.

2) If $m_1=m_2=m$,and there doesn't exist $g_x(x)$ which makes $g_x(x)=g_2(x)$ or $g_x(x)=1+g_2(x)$, and g_x is an annihilator of the lowest algebraic degree of $f_1(x)$,

a. If m-degree terms of $g_1(x)$ and $g_2(x)$ are unequal, or at least one m-degree term is unequal in many m-degree terms, $AI(f(x))=m+1$.

b. If all the m-degree terms of $g_1(x)$ and $g_2(x)$ are equal, but the second high-degree terms are unequal, or at least one of many second high-degree terms is unequal, $AI(f(x))=m$.

Remark: The results of Theorem 1 are based on the Definition 3 of cascade in this paper.

For the proof of Theorem 1, attention should only be paid that we should take $(0\|g_2(x))f(x)=0$ (or $(0\|g_2(x))(1+f(x))=0$ correspondingly) in 1) of 2. Proofs of other clauses in Theorem 1 are easy, so we omit it here.

Theorem 2 will further discuss the existence of correlation immunity H Boolean functions whose algebraic immunity is not less than 2 (that $AI(f(x))\geq 2$), and the existence of the optimal algebraic immunity H Boolean functions with correlation immunity.

Theorem 2: $f(x)$ are H Boolean functions with $w_t(f(x))=2^{n-1}+2^{n-2}$. If $n\geq 5$,

$$w_t(\partial f(x)/\partial(x_{n-1}x_n))=2^{n-2}, \quad (5)$$

and

$$w_t(ef(x)/e(x_{n-1}x_n))=2^{n-1}+2^{n-3}. \quad (6)$$

Taking

$$\begin{aligned} &g(x) \\ &=\partial(f(x)df(x)/dx_n)/\partial(x_{n-1}x_n) \\ &+e(ef(x)/ex_n)/e(x_{n-1}x_n)(x_{n-1}+x_n) \\ &+e(f(x)df(x)/dx_n)/e(x_{n-1}x_n) \end{aligned}, \quad (7)$$

then we can get

1) There are

$$\begin{aligned} &f(x) \\ &=g(x)f(x)df(x)/dx_n \\ &+d(g(x)ef(x)/ex_n)/dx_n \end{aligned}, \quad (8)$$

and

$$\begin{cases} w_t(g(x))=2^{n-1} \\ eg(x)/ex_n=0 \end{cases}. \quad (9)$$

2) $g(x)$ is an annihilator of the lowest algebraic degree of $1+f(x)$.

3) If $w_t(\partial g(x)/\partial(x_{n-3}x_{n-2}x_{n-1}x_n))=2^{n-1}$, $AI(f)\geq 2$.

4) When $n\geq 5$, there exists the optimal algebraic immunity functions. If we can construct more than four(or three3) n-dimensional optimal algebraic immunity functions, and highest-degree terms of

annihilators g of any two optimal algebraic immunity functions are equal, the second high-order terms of $g_1(x)$, $g_3(x)$ and $g_4(x)$ are not absolutely equal, we can construct $n+2$-dimensional optimal algebraic immunity functions.

5) In $f(x)$ satisfy $AI(f) \geq 2$, there exist functions with $CI(f)=1$.

Proof: 1)

$$\begin{aligned} &dg(x)/dx_n \\ &= d(\partial(f(x)df(x)/dx_n)/\partial(x_{n-1}x_n))/dx_n \\ &+(x_{n-1}+x_n)d(e(ef(x)/ex_n)/e(x_{n-1}x_n))/dx_n \\ &+e(ef(x)/ex_n)/e(x_{n-1}x_n)d(x_{n-1}+x_n)/dx_n \\ &+d(e(f(x)df(x)/dx_n)/e(x_{n-1}x_n))/dx_n \end{aligned} . \quad (10)$$

Since (5),(6), $w_t(f(x)) = 2^{n-1}+2^{n-2}$ and $w_t(df(x)/dx_i) = 2^{n-1}$ $(i=1,2,\cdots,n)$,we can know, if we equally divide the range of value $0 \sim 2^{n-1}$ of independent variable x into small ranges of value,which the numbers of 2^{n-2}:

$$0 \sim 2^2-1, 2^2 \sim 2^3-1, \cdots\cdots, 2^n-2^2 \sim 2^n-1. \quad (11)$$

The 2-variable function which is divided by $f(x)$ in the small range of value of (11) would be

$$\begin{cases} g_{01} = x_{n-1}+x_n \ and \ g_{02}=1 \\ g_{11} = 1+x_n+x_{n-1}x_n \ and \ g_{12} = 1+x_{n-1}+x_{n-1}x_n \end{cases} . \quad (12)$$

In (12), $g_{01}(x)$ and $g_{02}(x)$ must appear in pairs.

So we can know, in (10), there must be $d(e(ef(x)/ex_n)/e(x_{n-1}x_n))/dx_n = 0$. Moreover there must be

$$\begin{aligned} &dg(x)/dx_n = \\ &d(\partial(f(x)df(x)/dx_n)/\partial(x_{n-1}x_n))/dx_n \\ &+e(ef(x)/ex_n)/e(x_{n-1}x_n) \\ &+d(e(f(x)df(x)/dx_n)/e(x_{n-1}x_n))/dx_n \\ &=1 \end{aligned} , \quad (13)$$

and $dg(x)/dx_{n-1}=1$.

So

$$\begin{aligned} &d(g(x)ef(x)/ex_n)/dx_n \\ &= ef(x)/ex_n dg(x)/dx_n \\ &+g(x)d(ef(x)/ex_n)/dx_n \\ &+dg(x)/dx_n d(ef(x)/ex_n)/dx_n \\ &= ef(x)/ex_n \end{aligned} . \quad (14)$$

Because

$$\begin{aligned} &d(g(x)f(x)df(x)/dx_n)/dx_n = \\ &f(x)df(x)/dx_n dg(x)/dx_n \\ &+g(x)d(f(x)df(x)/dx_n)/dx_n \\ &+dg(x)/dx_n d(f(x)df(x)/dx_n)/dx_n \\ &= f(x)df(x)/dx_n + g(x)(df(x)/dx_n \\ &+f(x)d(df(x)/dx_n)/dx_n \\ &+df(x)/dx_n d(df(x)/dx_n)/dx_n) \\ &+dg(x)/dx_n d(f(x)df(x)/dx_n)/dx_n \\ &= f(x)df(x)/dx_n + g(x)df(x)/dx_n \\ &+df(x)/dx_n \\ &= (1+g(x)+f(x))df(x)/dx_n \end{aligned} , \quad (15)$$

we can get

$$\begin{aligned} &f(x)df(x)/dx_n d(g(x)f(x)df(x)/dx_n)/dx_n \\ &= g(x)f(x)df(x)/dx_n \end{aligned} . \quad (16)$$

Due to $e(f(x)df(x)/dx_n)/ex_n = 0$,

$$e(g(x)f(x)df(x)/dx_n)/ex_n = 0. \quad (17)$$

Therefore, thanks to (15) and (17), there is

$$\begin{aligned} &g(x)f(x)df(x)/dx_n \\ &= g(x)f(x)df(x)/dx_n d(g(x)f(x)df(x)/dx_n)/dx_n \\ &+e(g(x)f(x)df(x)/dx_n)/ex_n \\ &= g(x)f(x)df(x)/dx_n d(g(x)f(x)df(x)/dx_n)/dx_n \end{aligned} . \quad (18)$$

Known by (16) and (18),there is

$$\begin{aligned} &(f(x)df(x)/dx_n + g(x)f(x)df(x)/dx_n)\cdot \\ &d(g(x)f(x)d(g(x)f(x)df(x)/dx_n)/dx_n \\ &=0 \end{aligned} . \quad (19)$$

By (7), there is

$$\begin{aligned} &g(x)f(x)df(x)/dx_n \\ &= \partial(f(x)df(x)/dx_n)/\partial(x_{n-1}x_n)f(x)df(x)/dx_n \\ &+e(ef(x)/ex_n)/e(x_{n-1}x_n)(x_{n-1}+x_n)f(x)df(x)/dx_n \\ &+e(f(x)df(x)/dx_n)/e(x_{n-1}x_n)f(x)df(x)/dx_n \\ &\neq 0 \end{aligned} . \quad (20)$$

By (20) and (18),we have

$$\begin{cases} g(x)f(x)df(x)/dx_n d(g(x)f(x)df(x)/dx_n)/dx_n \\ \neq 0 \\ f(x)df(x)/dx_n d(g(x)f(x)df(x)/dx_n)/dx_n \neq 0 \end{cases} .$$

Hence we can know that both $g(x)f(x)df(x)/dx_n$ and $f(x)df(x)/dx_n$ are not the annihilators of $d(g(x)f(x)df(x)/dx_n)/dx_n$. So from (18),(20) and (19),there must be

$$g(x)f(x)df(x)/dx_n = f(x)df(x)/dx_n. \quad (21)$$

By (14),(21) and Lemma 2,we have

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

that is,(8) is established.

Since $dg(x)/dx_n = 1$ in (13), $\begin{cases} w_t(g(x)) = 2^{n-1} \\ eg(x)/ex_n = 0 \end{cases}$. That is,(9) is established too.

2) By (12),we have

$$\begin{aligned} &\partial g(x)/\partial(x_{n-1}x_n) \\ &= \partial(\partial(f(x)df(x)/dx_n)/\partial(x_{n-1}x_n))/\partial(x_{n-1}x_n) \\ &+\partial(x_{n-1}+x_n)/\partial(x_{n-1}x_n)e(ef(x)/ex_n)/e(x_{n-1}x_n) \\ &+(x_{n-1}+x_n)\partial(e(ef(x)/ex_n)/e(x_{n-1}x_n))/\partial(x_{n-1}x_n) \\ &+\partial(x_{n-1}+x_n)/\partial(x_{n-1}x_n)\partial(e(ef(x)/ex_n)/ \\ &e(x_{n-1}x_n))/\partial(x_{n-1}x_n) \\ &+\partial(e(f(x)df(x)/dx_n)/e(x_{n-1}x_n))/\partial(x_{n-1}x_n) \\ &=0 \end{aligned} \tag{22}$$

Since (9) is established, which means $w_t(g(x)) = 2^{n-1}$ and $eg(x)/ex_n = 0$. By (22),we can know

$$\begin{aligned} &eg(x)/e(x_{n-1}x_n) \\ &= g(x) + g(x)\partial g(x)/\partial(x_{n-1}x_n) = g(x) \end{aligned}. \tag{23}$$

By (9),(22) and (23),we can get 2-variable functions of the numbers of 2^{n-2} ,which are gotten after dividing $g(x)$ in the small range of value of (11),there are only

$$h_1 = x_{n-1} + x_n \quad and \quad h_2 = 1 + x_{n-1} + x_n . \tag{24}$$

Moreover by (7),we can know, $g(x)$ should only take $x_{n-1} + x_n$ in $ef(x)/ex_n$ to guarantee the degree won't add owing to the difference of cascade functions in concatenation.

By (23) and (21),we have

$$d(g(x) + f(x)df(x)/dx_n)/dx_n = ef(x)/ex_n . \tag{25}$$

And

$$\begin{cases} d(f(x)df(x)/dx_n)/dx_n = df(x)/dx_n \\ ef(x)/ex_n + df(x)/dx_n = 1 \end{cases}, \tag{26}$$

by (7),(12) and (23)~(26),we can know, in each small range of (11), $g(x)$ is concatenated of the same or complementary 1st-degree functions, and there is $\deg(h_1(x)\|h_2(x)) = \deg(x_{n-2} + x_{n-1} + x_n) = 1$. But for $ef(x)/ex_n$, there is $0\|x_{n-1}$, thus there exists $\deg(0\|x_{n-1}) = \deg(x_{n-2}x_{n-1}) = 2 > \deg(h_1(x)\|h_2(x))$.

Known by (23),(25) and (26),

$$\deg ef(x)/ex_n = \deg df(x)/dx_n > \deg g(x) . \tag{27}$$

Since $g(x)$ is certain for each $f(x)$,and it's concatenated of completely the same 1st-degree functions. So known by (27), $g(x)$ is an annihilator of the lowest algebraic degree of $1 + f(x)$.

3) Known By (12) and the condition $w_t(\partial g(x)/\partial(x_{n-3}x_{n-2}x_{n-1}x_n)) = 2^{n-1}$, if dividing $f(x)$ into concatenations of 5-variable functions, $g_5(x)$ which is the annihilator of the lowest algebraic degree of 5-variable functions is concatenated of $g_{41}(x)$ and $g_{42}(x)$ which are annihilators of the lowest algebraic degree of two 4-variable functions,which means $g_5(x) = g_{41}(x)\|g_{42}(x)$, and $g_{41}(x) \neq g_{42}(x)$. So

$$\deg g_5(x) \geq 2 . \tag{28}$$

But there must be $AI(f) \leq \left\lceil \frac{n}{2} \right\rceil$. So there is $\deg g_5(x) = \left\lceil \frac{5}{2} \right\rceil = 2$,which means there exist the optimal algebraic immunity functions.

Since (28),we can know,the annihilators of $f(x)$ also have $\deg g(x) \geq 2$.

Therefore,we can know that $AI(f(x)) \geq 2$.

4) Suppose n-dimensional functions $f_1(x)$, $f_2(x)$, $f_3(x)$ and $f_4(x)$ are all optimal algebraic immunity functions, $g_1(x)$, $g_2(x)$, $g_3(x)$ and $g_4(x)$ which are gotten by (7) are annihilators of $f_1(x)$, $f_2(x)$, $f_3(x)$ and $f_4(x)$ respectively, and

$$\begin{cases} f_1(x)\|f_2(x) \neq f_3(x)\|f_4(x) \\ (\texttt{or taking } f_4(x) = f_1(x)) . \\ g_1(x)\|g_2(x) \neq g_3(x)\|g_4(x) \end{cases} \tag{29}$$

And the highest degree terms of $g_1(x)$, $g_2(x)$, $g_3(x)$ and $g_4(x)$ are equal, the second high-degree term of $g_2(x)$ and the second high-order terms of $g_1(x)$, $g_3(x)$ and $g_4(x)$ are not absolutely equal, and $g_3(x) = 1 + g_4(x)$.

For $n+2$ -dimensional functions $f(x)$, $f(x) = f_1(x)\|f_2(x)\|f_3(x)\|f_4(x)$, known by 2 and 3 of Theorem 2, $f(x)$ have annihilators of the lowest algebraic degree $g(x)$, $g(x) = g_1(x)\|g_2(x)\|g_3(x)\|g_4(x)$. Then

$$\begin{cases} \deg(g_1(x)\|g_2(x)) = \deg g_1(x) = \deg g_2(x) = \left\lceil \frac{n}{2} \right\rceil \\ \deg(g_3(x)\|g_4(x)) = \deg g_3(x) = \deg g_4(x) = \left\lceil \frac{n}{2} \right\rceil \end{cases} \tag{30}$$

So known by (29) and (30), the highest degree term of $g_1(x)\|g_2(x)$ and $g_3(x)\|g_4(x)$ are unequal. And known from Theorem 1,

$$\begin{aligned} &\deg g(x) \\ &= \deg(g_1(x)\|g_2(x)\|g_3(x)\|g_4(x)) \\ &= \left\lceil \frac{n}{2} \right\rceil + 1 \\ &= \left\lceil \frac{n+2}{2} \right\rceil \end{aligned} .$$

That is, $f(x)$ is a $n+2$ -dimensional optimal algebraic immunity function.

5) Since the 2-variable functions $g_{01}(x) = x_{n-1} + x_n$ and $g_{02}(x) = 1$ are matched (appearing in pairs of function $f_1(x)$ and $f_2(x)$,denoted by $f_1 \circ f_2$),there is

$$\begin{aligned} & w_t(g_{01} \circ g_{02} \mid x_i = 0) \\ & = w_t(g_{01} \circ g_{02} \mid x_i = 1) \ (i = n-1, n). \\ & = 2^{-1} w_t(g_{01} \circ g_{02}) \end{aligned} \quad (31)$$

For the $g_{11} \circ g_{12}$ which means $g_{11} = 1 + x_n + x_{n-1}x_n$ and $g_{12} = 1 + x_{n-1} + x_{n-1}x_n$ have been match, there also be

$$\begin{aligned} & w_t(g_{11} \circ g_{12} \mid x_i = 0) \\ & = w_t(g_{11} \circ g_{12} \mid x_i = 1) \ (i = n-1, n). \\ & = 2^{-1} w_t(g_{11} \circ g_{12}) \end{aligned} \quad (32)$$

In H Boolean functions with $w_t(f(x)) = 2^{n-1} + 2^{n-2}$, $g_{01} \circ g_{02}$ is necessary.Otherwise,it doesn't satisfy the weight condition of Boolean Functions and the request of $w_t(df(x)/dx_i) = 2^{n-1}$ $(i = 1, 2, \cdots, n)$. So we only need to require g_{11} and g_{12} in $f(x)$ to appear in pairs too.Thus,by (31) and (32), there must be

$$\begin{aligned} & w_t(f(x) \mid x_i = 0) \\ & = w_t(f(x) \mid x_i = 1) = 2^{-1} w_t(f(x)) \end{aligned} \quad (i = 1, 2, \cdots, n).$$

So we can know, there is existence of functions $f(x)$ which with $AI(f(x)) \geq 2$ and $CI(f(x)) = 1$.

The proof ends.

From the proof of 4) and 5) in Theorem 2,we can obtain the following Corollary 1.

Corollary 1: In H Boolean function $f(x)$ with $w_t(f(x)) = 2^{n-1} + 2^{n-2}$, there exists the optimal algebraic immunity functions with correlation immunity.

4 Conclusions

Using 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(the amount and the distribution of the values of two different properties). In the 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 many problems of cryptographic properties of Boolean functions using the derivative and 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.

Acknowledgment

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. L. Qu, C. Li. On the 2^m -variable symmetric Boolean functions with maximum algebraic immunity. Science in China Series F: Information Sciences, 2008, 51, (2), pp. 120-127.
3. L. Qu, C. Li, K. Feng. A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables. IEEE Transactions on Information Theory, 2007, 53, (8), pp. 2908-2910.
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, 2011, 60, (1), pp. 1-14.
5. Q. Wang, J. Peng, H. Kan, X. Xue. Constructions of cryptographically significant Boolean functions using primitive polynomials. IEEE Transactions on Information Theory, 2010, 56, (6), pp. 3048-3053.
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, 2011, 57, (10), pp. 7205-7220.
7. J. Huang, Z. Wang. The relationship between correlation immune and weight of H Boolean functions. Journal on Communications, Vol.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, Vol.40(5-6):905-911(2011).
9. Y. Ding, Z. Wang, J. Ye. Initial-value problem of the Boolean function's primary function and its application in cryptographic system. Kybernetes, Vol.39(6): 900-906(2010).