Applied Mechanics and Materials *Online: 2013-10-31*
ISSN: 1662-7482, Vol. 459, pp 195-200
doi:10.4028/www.scientific.net/AMM.459.195

The Judgment of Algebraic Immunity and Resilience of Balanced H Boolean Functions

Jinglian Huang[1,a], Zhuo Wang[1,b], Yajing Liu[2,c]

[1]School of Computer Science and Information Engineering, Northwest University for Nationalities, Lanzhou, P.R.China

[2]School of Business, East China University of Science and Technology, Shanghai, P.R.China

[a]huangjlwork@163.com, [b]wzh0902@126.com, [c]ya_jingliu@126.com

Keywords: Balanced H Boolean function; E-derivative; Algebraic immunity; Resilience; Judgment

Abstract. Using the derivative of the Boolean function and the e-derivative defined by ourselves as main research tools, we study the relationship among e-derivative, algebraic immunity and resilience of balanced H Boolean functions.We get some theorems which connect algebraic immunity, annihilators, resilience, derivative and e-derivative of balanced H Boolean functions together. Besides, we also get the judgment of algebraic immunity and resilience for three classes of balanced Boolean functions by the e-derivative.

Introduction

In recent years,several successful algebraic attacks on stream ciphers have been proposed.To resist this kind of attacks,a new cryptographic property of Boolean functions called algebraic immunity was introduced by Meier *et al*. [1].The Boolean function used in a cryptosystem should have good cryptographic properties such as balance, high correlation immunity, high algebraic degree, high algebraic immunity, resilience and high nonlinearity.These properties are required to resist many kinds of known attacks [2,3]. In the study of the algebraic immunity and other cryptography properties of Boolean functions,the main research methods we take are as follows. For instance, the methods of recursively definition and cascade calculation, proceeding from a Boolean function with optimum algebraic immunity, it is easy to construct another Boolean function with optimum algebraic immunity, and the trace representation based Boolean functions,track division.There are some methods such as the zero set, the support set and *k*-dimensional subspace of the zero set, the weight support technique,and algorithms of annihilators set. The above methods need do multi-step calculations step-by-step to obtain the results, which are more complicated.In this paper,using the derivative of the Boolean function and the e-derivative defined by ourselves as main research tools, we go deep into the internal structure of the Boolean function values, studying the judgment of algebraic immunity and resilience of balanced H Boolean Functions.

From reference [4], it is known that, the e-derivative plays the important role to differentiate correlation immunities according to the different weights of Boolean functions. Therefore, it is natural to expect that the e-derivative could further help to unify the algebraic immunity and the resilient. This would be a hint for the trial of our later discussions.

Preliminaries

The derivative of Boolean functions is known by people [5~8]. The e-derivative of the Boolean function is given below. The relationships of the e-derivative and derivative and properties of e-derivative, can be known from references [4, 9~11].

Definition 1*:* The e-derivative (e-partial derivative) of Boolean function $f(x_1, x_2, \cdots, x_n)$ with respect to *r* variables $x_{i1}, x_{i2}, \cdots, x_{ir}$ $(i, r \in [1, n])$ is defined as

$$ef(x)/e(x_{i1}, x_{i2}, \cdots, x_{ir}) = f(x_1, x_2, \cdots, x_{i1}, x_{i2}, \cdots, x_{ir}, \cdots, x_n) f(x_1, x_2, \cdots, 1+x_{i1}, 1+x_{i2}, \cdots, 1+x_{ir}, \cdots, x_n) \quad (1)$$

If $r=1$, (1) turns into the e-derivative with respect to 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.

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

Lemmas 1~4 that follow describe the properties of derivative and e-derivative of Boolean functions and balanced H Boolean functions.

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

$$w_t(\partial f(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir}))=2^{n-1}\ (1\le i\le n,1\le r\le n,1\le i_1\le i_2\le\cdots\le i_r\le n) \tag{3}$$

Lemma 2: A Boolean function is an H Boolean function iff the following equations hold for all x_i:

$$w_t(df(x)/dx_i)=2^{n-1}\ (i=1,2,\cdots,n) \tag{4}$$

Lemma 3: For any arbitrary Boolean function, the following equations are true:

$$f(x)=f(x)\partial f(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir})+ef(x)/e(x_{i1},x_{i2},\cdots,x_{ir})\ (1\le i\le n,1\le r\le n,1\le i_1\le i_2\le\cdots\le i_r\le n) \tag{5}$$

$$f(x)=f(x)df(x)/dx_i+ef(x)/ex_i\ (i=1,2,\cdots,n) \tag{6}$$

$$w_t(f(x))=w_t(f(x)df(x)/dx_i)+w_t(ef(x)/ex_i)=2^{-1}w_t(df(x)/dx_i)+w_t(ef(x)/ex_i)\ (i=1,2,\cdots,n) \tag{7}$$

Lemma 4: A Boolean function $f(x)$ is a balanced H Boolean function iff

$$w_t(df(x)/dx_i)=2^{n-1}\text{ and }w_t(ef(x)/ex_i)=2^{n-2}\ (i=1,2,\cdots,n) \tag{8}$$

Definition 2: If $w_t(f(x))=r\ne 0$, suppose that $g(1+f)=0$ and $w_t(g)=s\le r$, then function g is called a sub-function of function f with $gf=g$. Evidently, g is an annihilator of $1+f$, and any sub-function of $1+f$ is also annihilator of f.

The judgment of algebraic immunity and resilience of balanced H Boolean functions

In this section,we discuss the judgment of algebraic immunity and resilience of balanced Boolean functions by the e-derivative. Firstly,a theorem is introduced here about the relationship among resilient H Boolean functions, e-derivative and derivative of balanced H Boolean functions.

Theorem 1: $f(x)$ are balanced H Boolean functions, for any x_i $(i=1,2,\cdots,n)$, there are

$$w_t(x_i ef(x)/ex_k)=2^{-1}w_t(ef(x)/ex_k)=2^{n-3}\ (i\ne k,k=1,2,\cdots,n) \tag{9}$$

and

$$w_t(x_i f(x)df(x)/dx_k)=2^{-1}w_t(f(x)df(x)/dx_k)=2^{n-3}\ (i\ne k,k=1,2,\cdots,n) \tag{10}$$

then $f(x)$ are $(n,1,1)$-resilient H Boolean functions.

Proof: For any x_i $(i=1,2,\cdots,n)$, there are

$$w_t(d(f(x)+x_i)/dx_k)=w_t(df(x)/dx_k)=2^{n-1}\ (i\ne k,k=1,2,\cdots,n) \tag{11}$$

$$\begin{aligned} &w_t(e(f(x)+x_i)/ex_k)\\ &=w_t(ef(x)/ex_k+x_i df(x)/dx_k+x_i) \qquad (i\ne k,k=1,2,\cdots,n)\\ &=w_t(ef(x)/ex_k)+w_t(x_i df(x)/dx_k)+w_t(x_i)-2w_t(x_i ef(x)/ex_k)-2w_t(x_i df(x)/dx_k)\end{aligned} \tag{12}$$

Known by (11),(12) and Lemmas 3, $f(x)$ have correlation immunity iff

$$2^{-1}w_t(df(x)/dx_k)+w_t(ef(x)/ex_k)-2w_t(x_i ef(x)/ex_k)-w_t(x_i df(x)/dx_k)+w_t(x_i)=2^{n-1} \tag{13}$$

By Lemmas 3,we can know that $f(x)$ have correlation immunity iff

$$\begin{aligned} &w_t(f(x)df(x)/dx_k+ef(x)/ex_k+x_i)\\ &=w_t(f(x)df(x)/dx_k)-2w_t(x_i f(x)df(x)/dx_k)+w_t(ef(x)/ex_k)-2w_t(x_i ef(x)/ex_k)+w_t(x_i)=2^{n-1}\\ &(i\ne k,k=1,2,\cdots,n)\end{aligned} \tag{14}$$

There is also

$$\begin{aligned} &d(f(x)df(x)/dx_k)/dx_k\\ &=df(x)/dx_k+f(x)d(df(x)/dx_k)/dx_k+df(x)/dx_k d(df(x)/dx_k)/dx_k=df(x)/dx_k\end{aligned} \tag{15}$$

So we can get

$$w_t(f(x)df(x)/dx_k)=2^{-1}w_t(df(x)/dx_k)\ (k=1,2,\cdots,n) \tag{16}$$

Solving simultaneous equations which are established by multiplying formula (13),(14) and (16), we can obtain

$$w_t(x_i df(x)/dx_k) = 2w_t(x_i f(x) df(x)/dx_k) \ (i \neq k, k = 1,2,\cdots,n) \tag{17}$$

If taking

$$w_t(ef(x)/ex_k) = 2w_t(x_i ef(x)/ex_k) \ (i \neq k, k = 1,2,\cdots,n) \tag{18}$$

By (18) and (14),we have

$$w_t(f(x)df(x)/dx_k) = 2w_t(x_i f(x) df(x)/dx_k) \ (i \neq k, k = 1,2,\cdots,n) \tag{19}$$

By (18) and (13),we have

$$w_t(df(x)/dx_k) = 2w_t(x_i df(x)/dx_k) \ (i \neq k, k = 1,2,\cdots,n) \tag{20}$$

Therefore,we can get that if (18) and (19) establish, (14) must establish, $f(x)$ must be correlation immune functions. And if (18) and (20) establish, (13) must establish, $f(x)$ must be correlation immune functions.Hence,if (9) and (10) establish, balanced H Boolean Functions $f(x)$ must be correlation immune functions. $f(x)$ are $(n,1,1)$-resilient H Boolean functions as well.

We will discuss the algebraic immunity of $(n,1,1)$-resilient H Boolean functions as follows.

Theorem 2: If balanced H Boolean functions $f(x)$ satisfy

$$\partial f(x)/\partial(x_{n-3}x_{n-2}x_{n-1}x_n) = 0 \tag{21}$$

$$df(x)/dx_{n-4} = 1 + df(x)/dx_{n-2} \tag{22}$$

$$\partial f(x)/\partial(x_{n-1}x_n) = 1 \tag{23}$$

We can get

1. $g_1(x) = e(1+f(x))/ex_n$ and $g_2(x) = (1+f(x))df(x)/dx_n$ are two annihilators of the lowest algebraic degree of $f(x)$, $g_3(x) = ef(x)/ex_n$ and $g_4(x) = f(x)df(x)/dx_n$ are two annihilators of the lowest algebraic degree of $1+f(x)$,as well as

$$\begin{cases} \deg g_1(x) = \deg g_2(x) = \deg g_3(x) = \deg g_4(x) = 2 \\ AI(f(x)) = 2 \end{cases} \tag{24}$$

2. $f(x)$ are $(n,1,1)$-resilient H Boolean functions.

Proof: 1. Because $f(x)$ are balanced H Boolean functions, there are

$$w_t(1+f(x)) = 2^n - w_t(f(x)) = 2^{n-1} \tag{25}$$

$$w_t(d(1+f(x))/dx_i) = w_t(df(x)/dx_i) = 2^{n-1} \ (i = 1,2,\cdots,n) \tag{26}$$

So,we can get that $1+f(x)$ are balanced H Boolean functions too.

Since $f(x)$ satisfy (21) and (23),there are

$$\partial(1+f(x))/\partial(x_{n-3}x_{n-2}x_{n-1}x_n) = \partial 1/\partial(x_{n-3}x_{n-2}x_{n-1}x_n) + \partial f(x)/\partial(x_{n-3}x_{n-2}x_{n-1}x_n) = 0 \tag{27}$$

$$\partial(1+f(x))/\partial(x_{n-1}x_n) = \partial 1/\partial(x_{n-1}x_n) + \partial f(x)/\partial(x_{n-1}x_n) = 1 \tag{28}$$

By calcluating,we can get

$$\begin{cases} d(1+f(x))/dx_{n-4} = df(x)/dx_{n-4} \\ d(1+f(x))/dx_{n-2} = df(x)/dx_{n-2} \end{cases} \tag{29}$$

Known by (29) and (22),we have

$$d(1+f(x))/dx_{n-4} = 1 + d(1+f(x))/dx_{n-2} \tag{30}$$

Known by (25) and (26),we have

$$w_t(e(1+f(x))/ex_n) = 2^{n-2} \tag{31}$$

Known by (28),(25),(26) and (31),we have

$$\begin{cases} e(e(1+f(x))/ex_n)/ex_{n-1} = 0 \\ \deg(d(e(1+f(x))/ex_n)/dx_{n-1}) = 1 \end{cases} \tag{32}$$

According to (22),(23) and (32), one knows that

$$\deg(d(e(1+f(x))/ex_n)/dx_i) = 1 \ \ (i = 1,2,\cdots,n-2) \tag{33}$$

So by (32) and (33),we can get

$$\deg(e(1+f(x))/ex_n) = 2 \tag{34}$$

Known from (28),(32) and (34),there are

$$\partial(e(1+f(x))/ex_n)/\partial(x_{n-1}x_n)\partial((1+f(x))d(1+f(x))/dx_n)/\partial(x_{n-1}x_n)=0 \tag{35}$$

$$\partial(e(1+f(x))/ex_n)/\partial(x_{n-1}x_n)+\partial((1+f(x))d(1+f(x))/dx_n)/\partial(x_{n-1}x_n)=1 \tag{36}$$

So by (35) and (36),we can get

$$\begin{aligned} &d(\partial((1+f(x))d(1+f(x))/dx_n)/\partial(x_{n-1}x_n))/dx_{n-2} \\ &=\partial(\partial((1+f(x))d(1+f(x))/dx_n)/\partial(x_{n-1}x_n))/\partial(x_{n-2}x_{n-1}x_n)=1 \end{aligned} \tag{37}$$

$$\deg((1+f(x))d(1+f(x))/dx_n)=2 \tag{38}$$

And known by (33) and (37), $g_1(x)=e(1+f(x))/ex_n$ and $g_2(x)=(1+f(x))df(x)/dx_n$ are two annihilators of the lowest algebraic degree of $f(x)$.

Since the condition (21)~(23) which are satisfied by $f(x)$ are similar with the condition (27),(30) and (28) which are satisfied by $1+f(x)$, by the same deduction of the above proof ,we can get: $g_3(x)=ef(x)/ex_n$ and $g_4(x)=f(x)df(x)/dx_n$ are two annihilators of the lowest algebraic degree of $1+f(x)$,and

$$\deg ef(x)/ex_n=\deg f(x)df(x)/dx_n=2 \tag{39}$$

So $AI(f(x))=2$.

2. According to (21)~(23),and the deduction of (35) and (36),we can get

$$\partial(ef(x)/ex_n)/\partial(x_{n-1}x_n)\partial(f(x)df(x)/dx_n)/\partial(x_{n-1}x_n)=0 \tag{40}$$

$$\partial(ef(x)/ex_n)/\partial(x_{n-1}x_n)+\partial(f(x)df(x)/dx_n)/\partial(x_{n-1}x_n)=1 \tag{41}$$

Known by (23),(40) and (41),there must be

$$\begin{cases} w_t(x_i ef(x)/ex_n)=2^{-1}w_t(ef(x)/ex_n)=2^{n-3} \\ w_t(x_i f(x)df(x)/dx_n)=2^{-1}w_t(f(x)df(x)/dx_n)=2^{n-3} \end{cases} (i=1,2,\cdots,n) \tag{42}$$

Therefore, according to Theorem 1 and (42),we can get that balanced H Boolean function $f(x)$ are correlation immune functions. So $f(x)$ are $(n,1,1)$-resilient H Boolean functions.

Theorem 3: If balanced H Boolean functions $f(x)$ satisfy

$$\partial f(x)/\partial(x_{n-2}x_{n-1}x_n)=0 \tag{43}$$

$$w_t(f(x)ef(x)/e(x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n))=2^{n-2}+2^{n-3} \tag{44}$$

$$w_t(f(x)\partial f(x)/\partial(x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n))=2^{n-3} \tag{45}$$

$$\partial(ef(x)/ex_n)/\partial(x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n)=0 \tag{46}$$

We can get

1. $ef(x)/ex_n$ is an annihilator of the lowest algebraic degree of $1+f(x)$, $e(1+f(x))/ex_n$ is an annihilator of the lowest algebraic degree of $f(x)$,and

$\deg ef(x)/ex_n=\deg e(1+f(x))/ex_n=2$

2. $f(x)$ are $(n,1,1)$-resilient H Boolean functions.

Proof: 1. Since $f(x)$ are balanced H Boolean functions, there are

$$w_t(f(x))=2^{n-1}, w_t(df(x)/dx_n)=2^{n-1}, w_t(f(x)df(x)/dx_n)=2^{n-2}, w_t(ef(x)/ex_n)=2^{n-2} \tag{47}$$

According to (43),(46) and (47),there must be

$$\partial(ef(x)/ex_n)/\partial(x_{n-1}x_n)=d(ef(x)/ex_n)/dx_{n-1} \tag{48}$$

$$w_t(d(ef(x)/ex_n)/dx_{n-1})=2^{n-1} \tag{49}$$

Known by (48),(49) and (44)~(46),we have

$$d(d(ef(x)/ex_n)/dx_{n-1})/dx_{n-3}=1 \tag{50}$$

So there is

$$\deg(\partial(ef(x)/ex_n)/\partial(x_{n-1}x_n))=\deg d(ef(x)/ex_n)/dx_{n-1}=1 \tag{51}$$

According to (48) and (44)~(46),we can get

$$d(ef(x)/ex_n)/dx_{n-3}=d(ef(x)/ex_n)/dx_{n-4} \tag{52}$$

$$d(ef(x)/ex_n)/dx_{n-2}=d(ef(x)/ex_n)/dx_{n-1} \tag{53}$$

And

$$\begin{aligned} &e(d(ef(x)/ex_n)/dx_{n-3})/e(x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n) = e(d(ef(x)/ex_n)/dx_{n-3})/e(x_{n-3}x_{n-2}x_{n-1}x_n) \\ &= e(d(ef(x)/ex_n)/dx_{n-3})/e(x_{n-2}x_{n-1}x_n) = 0 \end{aligned} \tag{54}$$

Then by (52) and (54),we can get

$$\deg d(ef(x)/ex_n)/dx_{n-3} = \deg d(ef(x)/ex_n)/dx_{n-4} = 1 \tag{55}$$

And by (53) and (51),we can get

$$\deg d(ef(x)/ex_n)/dx_{n-2} = 1 \tag{56}$$

Since $f(x)$ are balanced H Boolean functions, there is

$$w_t(df(x)/dx_i) = 2^{n-1} \ (i = 1,2,\cdots,n) \tag{57}$$

Since $f(x)$ satisfy the condition (43)~(46) and the formula (57),there is

$$\begin{aligned} &d(ef(x)/ex_n)/dx_i \\ &= d(ef(x)/ex_n)/dx_{n-3} = d(ef(x)/ex_n)/dx_{n-4} \end{aligned} \quad (i = n-5, n-6,\cdots,3,2,1) \tag{58}$$

So according to (58) and (55), one can know that

$$\deg d(ef(x)/ex_n)/dx_i = 1 \ (i = n-5, n-6,\cdots,3,2,1) \tag{59}$$

according to (51),(55),(56) and (59),there is

$$\deg ef(x)/ex_n = 2 \tag{60}$$

And by (43)~(46),we can get that $ef(x)/ex_n$ is an annihilator of the lowest algebraic degree of $1+f(x)$.

Known by (43)~(46),there must be

$$\deg(e(1+f(x))/ex_n + ef(x)/ex_n) = \deg(d(ef(x)/ex_n)/dx_{n-3}) \tag{61}$$

and $e(1+f(x))/ex_n$ is an annihilator of the lowest algebraic degree of $f(x)$.

So according to (55) and (61), one knows that

$$\deg(e(1+f(x))/ex_n + ef(x)/ex_n) = 1 \tag{62}$$

Then according to (60) and (62),there must be

$$\deg e(1+f(x))/ex_n = 2 \tag{63}$$

Hence, $AI(f(x)) = 2$.

2. Known by (43), one knows that

$$w_t(f(x)\,|\,x_i = 0) = w_t(f(x)\,|\,x_i = 1) = 2^{-1}w_t(f(x)) \ (i = n-2, n-1, n) \tag{64}$$

So

$$w_t(x_i f(x)df(x)/dx_n) = 2^{-1}w_t(f(x)df(x)/dx_n) = 2^{n-3} \ (i = n-2, n-1, n) \tag{65}$$

$$w_t(x_i ef(x)/ex_n) = 2^{-1}w_t(ef(x)/ex_n) = 2^{n-3} \ (i = n-2, n-1, n) \tag{66}$$

According to (43)~(46),there must be

$$w_t(x_i f(x)df(x)/dx_n) = 2^{-1}w_t(f(x)df(x)/dx_n) = 2^{n-3} \ (i = 1,2,\cdots,n-3) \tag{67}$$

$$w_t(x_i ef(x)/ex_n) = 2^{-1}w_t(ef(x)/ex_n) = 2^{n-3} \ (i = 1,2,\cdots,n-3) \tag{68}$$

Then According to (65)~(68) and Theorem 1,we can get that balanced H Boolean functions $f(x)$ are correlation immune functions. So $f(x)$ are $(n,1,1)$-resilient H Boolean functions.

Using the similar proof of Theorem 3, we can get Theorem 4 which reveals the relationship between algebraic immunity of another class of $(n,1,1)$-resilient H Boolean functions and the e-derivative. Limited by the length,Theorem 4 is given as follows without proof.

Theorem 4: If balanced H Boolean functions $f(x)$ satisfy

$$\partial f(x)/\partial(x_{n-2}x_{n-1}x_n) = 0 \tag{69}$$

$$d(d(ef(x)/ex_n)/dx_{n-2})/dx_{n-4} = 1 \tag{70}$$

$$\partial f(x)/\partial(x_{n-4}x_{n-3}x_{n-2}x_{n-1}x_n) = 0 \tag{71}$$

We can get

1. $ef(x)/ex_n$ is an annihilator of the lowest algebraic degree of $1+f(x)$, $e(1+f(x))/ex_n$ is an annihilator of the lowest algebraic degree of $f(x)$,and

$$\begin{cases} \deg ef(x)/ex_n = \deg e(1+f(x))/ex_n = 2 \\ AI(f(x)) = 2 \end{cases}$$

2. $f(x)$ are $(n,1,1)$-resilient H Boolean functions.

Conclusions

The relationship of algebraic immunity,correlation immunity, annihilators and resilience is addressed for balanced H Boolean functions. It is shown that the most crucial factor that impacts and combines the above characteristics is the e-derivative. The research in this paper is fundamental and could be extended toward the problems on compatibility among the different cryptography properties of other types of H Boolean functions such as Bent functions and rotational symmetric functions. It can be seen that the e-derivative should also play an important role while dealing with the variant types of H Boolean functions. It should be the key to solve the concomitant problems.

Acknowledgment

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

Corresponding Author

Jinglian Huang, huangjlwork@163.com, 86-13909440966.

References

[1] W. Meier, E. Pasalic, C. Carle . Algebraic attacks and decomposition of Boolean functions. In Advances in Cryptology-EUROCRYPT 2004. LNCS 3027, Berlin: Springer-Verlag, 2004. 474-491.

[2] Ding C, Xiao G, Shan W. “The stability theory of stream ciphers”. LNCS. Berlin:Springer-Verlag, 1991, vol.561.

[3] C. Carlet, “Boolean functions for cryptography and error correcting codes, chapter of the monography,” *in Boolean Models and Methods in Mathematics,Computer Science and Engineering*, P. Hammer and Y. Crama,Eds. Cambridge,U.K.:Cambridge University Press, 2010, pp.257-397.

[4] 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)

[5] Q. Wen, X. Niu , Y. Yang. *The Boolean Functions in modern cryptology*. Beijing: Science Press (2000).

[6] G. Xiao, J. Massey. “A Spectral Characterization of Correlation-Immune Combining Functions”. *IEEE Trans. on Inform.Theory*. Vol.34(3): 569-571(1988).

[7] S. Li, B. Zeng, Y. Lian, et al. *Logical functions in cryptography*. Beijing: China National Computer Software and Technology Service Corporation Press (2003).

[8] Q. Wen, J. Zhang, X. Niu, Y. Yang. “Review of Boolean Functions of Modern Cryptography. *Telecommunication Science*,Vol.20(12):43-46 (2004). (In Chinese)

[9] 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).

[10] L. He, Z. Wang, W. Li. Algorithm of reducing the balanced H-Boolean function correlation-measure and research on correlation issue. *Journal on Communications*, Vol.31(2): 93-99 (2011). (In Chinese)

[11] 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).