The Annihilators and the Correlation Immunity of H Boolean Functions

Jinglian Huang\textsuperscript{a,*}, Zhuo Wang\textsuperscript{b}

School of Electrical Engineering, Northwest University for Nationalities, Lanzhou, China
\textsuperscript{a}huangjlwork@163.com, \textsuperscript{b}wzh0902@126.com

Keywords: H Boolean function, cryptographic properties, e-derivative, algebraic immunity, correlation immunity, annihilators.

Abstract. Using the derivative and the e-derivative defined by ourselves as research tools, we study the compatibility of algebraic immunity and correlation immunity of $H$ Boolean functions with Hamming weight of $2^{n-1} + 2^{n-2}$. We obtain the necessary conditions which the e-derivative satisfies and the necessary and sufficient conditions that the derivative part represents, when $H$ Boolean functions have $m$-order correlation immunity. We also arrive at the sufficient and necessary condition and the sufficient condition, which are the ones that $H$ Boolean functions satisfy the compatibility of 1st-order algebraic immunity and $m$-order correlation immunity using e-derivative and derivative. What is more, the main theoretical results are verified through example and are revealed to be correct.

1. Introduction

The cipher security is the core of the cryptosystem. 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].

On the study of cryptography properties of Boolean functions, the main research methods [1–6] we take are as follows, such as the methods of algebraic analysis, spectral analysis, matrix analysis, weighting analysis, linear subspace analysis and cascade analysis [1]. Using these methods, we analyze the whole values of Boolean functions, but cannot differentiate values of Boolean functions’ two different properties. Therefore we cannot find the relation between values of Boolean functions’ two different properties and properties of Boolean functions.

The derivative of Boolean function was proposed long ago [1]. The derivative of Boolean function doesn’t play a significant role when it is used alone in studying the properties of Boolean functions. Using the derivative of Boolean function expresses the values of one property of Boolean functions, and the values of another property of Boolean functions can be reflected by the e-derivative which defined by ourselves[7–8]. Using the derivative and the e-derivative as main research tools to study the cryptographic properties of Boolean functions, we can reveal the relation between values of Boolean functions’ two different properties and properties of Boolean functions, so we will find more useful results.

$H$ Boolean function is function with 1-degree propagation. In this paper, using the derivative and e-derivative as research tools, we study the compatibility of correlation immunity and algebraic immunity, and the relationships among algebraic immunity, correlation immunity, derivative and e-derivative of $H$ Boolean functions 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 \( f(x) = f(x_1, x_2, \ldots, x_n) \in GF(2)^{GF(2^r)} \) for \( r \) variables \( x_{i_1}, x_{i_2}, \ldots, x_{i_r} \) (\( i, r \in [1,n] \)) is defined as

\[
ef(x)/e(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) = f(x_1, x_2, \ldots, x_{i_1}, x_{i_2}, \ldots, x_{i_r})/e(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) = f(x_1, x_2, \ldots, x_{i_1}, x_{i_2}, \ldots, x_{i_r})/e(x_{i_1}, x_{i_2}, \ldots, x_{i_r})
\]

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

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

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

\[
ef(x)/\partial(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) = f(x_1, x_2, \ldots, x_{i_1}, x_{i_2}, \ldots, x_{i_r}) + f(x_1, x_2, \ldots, x_{i_1}, 1, x_{i_2}, \ldots, x_{i_r}) + f(x_1, x_2, \ldots, x_{i_1}, 0, x_{i_2}, \ldots, x_{i_r}) \quad (i = 1,2,\ldots,n).
\]

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

\[
df(x)/dx_i = f(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) + f(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \quad (i = 1,2,\ldots,n).
\]

Definition 3: For any arbitrary \( \omega = (\omega_1, \omega_2, \ldots, \omega_n) \in GF(2)^n \), \( 1 \leq \omega_i(\omega) \leq m \),

\[
f(x) = f(x_1, x_2, \ldots, x_n) \in GF(2)^{GF(2^r)} \) holds: \( w_i(f(x) + \omega x) = 2^{m-1} \) (\( \omega x \) is a linear function). In this situation, Boolean functions \( f(x) \) was called a \( m \)-order correlation immune function.

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

Lemma 1: A Boolean function \( f(x) \) is an H Boolean function iff the following equations hold for all \( x_i : w_i(df(x)/dx_i) = 2^{m-1} \) \( (i = 1,2,\ldots,n) \).

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

\[
f(x) = f(x)\partial f(x)/\partial(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) + ef(x)/e(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) \quad (1 \leq i \leq n, 1 \leq r \leq n, 1 \leq i_1 \leq i_2 \leq \cdots \leq i_r \leq n),
\]

and

\[
w_i(f(x)) = w_i(f(x)df(x)/dx_i) + w_i(ef(x)/ex_i) = 2^{m-1}w_i(df(x)/dx_i) + w_i(ef(x)/ex_i) \quad (i = 1,2,\ldots,n).
\]

Lemma 3: A Boolean function \( f(x) \in GF(2)^{GF(2^r)} \) with correlation immunity of order \( m \) \( (m \geq 1) \) iff, for \( \omega x \) \( (1 \leq w_i(\omega) \leq m) \), there exists \( w_i(\omega x f(x)) = 2^{m-1}w_i(f(x)).
\]

3. The Annihilators and the correlation immunity of H Boolean function

In this section, we reveal the relations between annihilators and correlation immunity of H Boolean function with \( w_i(f(x)) = 2^{m-1} + 2^{m-2} \), and the relations among e-derivative, derivative, algebraic immunity, correlation immunity and annihilators of H Boolean function with \( w_i(f(x)) = 2^{m-1} + 2^{m-2} \).

In Theorem 1, we discuss the relations between the e-derivative \( ef(x)/ex_i \) and \( \omega x \) \( (1 \leq w_i(\omega) \leq m) \) when \( f(x) \) is a \( m \)-order correlation immune H Boolean function with \( w_i(f(x)) = 2^{m-1} + 2^{m-2} \). Namely, we discuss the contact of e-derivative and correlation immunity of this class of H Boolean functions. We obtain the necessary condition which the e-derivative satisfies, if we want to get this kind of H Boolean functions with correlation immunity order \( m \).

Theorem 1: Suppose \( f(x) \) is an H Boolean function with \( w_i(f(x)) = 2^{m-1} + 2^{m-2} \) and that \( f(x) \) is correlation immune function of order \( m \). For \( x, \omega \in GF(2)^n \) \( (1 \leq w_i(\omega) \leq m) \), there is
\[ w_i(\omega x e(f(x)/e_i)) = 2^{n-2} \quad (i = 1, 2, \cdots, n). \] (3)

**Proof:** Making the affine function \( \omega x \).

1) When \( \omega x \) doesn’t contain \( x_i \), there are
\[ w_i(d(f(x) + \omega x) / dx_i) = w_i(\omega x f(x) / dx_i) = 2^{n-1} \] (4)
and
\[ w_i(\omega x (f(x) + \omega x) / ex_i) = w_i(\omega x (f(x) / ex_i) + \omega x df(x) / dx_i + \omega x) \\
= w_i(\omega x (f(x) / ex_i) + w_i(\omega x df(x) / dx_i) + w_i(\omega x) - 2w_i(\omega x (f(x) / ex_i + df(x) / dx_i))). \] (5)

Because \( w_i(f(x)) = 2^{n+1} + 2^{n-2} \), and \( f(x) \) is an H Boolean function. By Lemma 1&2, we can get
\[ ef(x) / ex_i + df(x) / dx_i = 1 \quad (i = 1, 2, \cdots, n). \] (6)
So
\[ \omega x (ef(x) / ex_i + df(x) / dx_i) = \omega x. \] (7)

By (7) and (5), we have
\[ w_i(\omega x f(x) / dx_i) = w_i(\omega x (f(x) / dx_i)) - w_i(\omega x). \] (8)

On account of \( w_i(f(x)) = 2^{n-1} + 2^{n-2} \), \( f(x) \) is an H Boolean function, and \( \omega x \) is an affine function. Then there are \( w_i(ef(x) / ex_i) = 2^{n-1} \quad (i = 1, 2, \cdots, n) \) and \( \omega x(\omega x) = 2^{n-1} \). Since \( 1 \leq w_i(\omega x) \leq m \), combine (4) with (8), we can know that \( f(x) \) is a correlation immune function of order \( m \). Then
\[ w_i(\omega x df(x) / dx_i) = 2^{n-2} \quad (\omega, x \in GF(2)^{\omega}, \omega x \) doesn't contain \( x_i, 1 \leq w_i(\omega x) \leq m, i = 1, 2, \cdots, n). \] (9)

Known by (6) and (9) is established. So
\[ w_i(\omega x (ef(x) / ex_i + df(x) / dx_i)) = 2^{n-2} \quad (\omega, x \in GF(2)^{\omega}, \omega x \) doesn't contain \( x_i, 1 \leq w_i(\omega x) \leq m, i = 1, 2, \cdots, n). \] (10)

2) When \( \omega x \) contain \( x_i \), there is
\[ w_i(d(ef(x) / ex_i + \omega x) / dx_i) = w_i(d(ef(x) / ex_i) / dx_i + d(\omega x) / dx_i) = w_i(0+1) = w_i(1) = 2^n. \]

We use \( h(0) \) as the symbol for \( x_i = 0 \) in \( \omega x \), and \( h(1) \) for \( x_i = 1 \) in \( \omega x \).
\[ w_i(\omega x (ef(x) / ex_i + \omega x) / ex_i) = w_i((ef(x) / ex_i + h(0))(ef(x) / ex_i + h(0))) \\
= w_i(ef(x) / ex_i + ef(x) / ex_i (h(0) + h(0) + h(0)h(1))) \\
= w_i(ef(x) / ex_i + ef(x) / ex_i \cdot 1+0) = 0 \]

By Lemma 2, we can get
\[ w_i(\omega x (ef(x) / ex_i + \omega x) / ex_i) = 2^{n-2} w_i(\omega x (ef(x) / ex_i + \omega x) / ex_i) = 2^{n-1}. \] (11)

Because
\[ w_i(ef(x) / ex_i + \omega x) = w_i(ef(x) / ex_i) + w_i(\omega x) - 2w_i(\omega x (ef(x) / ex_i)), \] (12)
by \( w_i(ef(x) / ex_i) = 2^{n-1}, w_i(\omega x) = 2^{n-1}, \) (11) and (12), there is
\[ w_i(\omega x (ef(x) / ex_i)) = 2^{n-2} \quad (\omega x \) contain \( x_i). \] (13)

Known by (13) and (10), for all \( \omega, x \in GF(2)^{\omega} \) \( (1 \leq w_i(\omega x) \leq m), \) (3) is established. The proof ends.

**Remark 1:** The (3) is the necessary condition for \( f(x) \) with correlation immunity of order \( m \) instead of the sufficient condition. For instance, if there is \( f(x) = 1 + x_n + x_{n-1} + x_{n-2} + x_{n-3} + x_{n-4} + x_{n-5} + x_{n-6} + x_{n-7} \), for \( \omega x = x_{n+1} + x_{n+2} + x_{n+3} \), we can get \( w_i(\omega x (ef(x) / ex_i)) = 2^{n-2} \). But owing to \( w_i(ef(x) / ex_i) = 2^{n-2} + 2^{n-3} \) and \( w_i(f(x) + x_n) = 2^{n-1} + 2^{n-3} \), so \( f(x) \) is not a correlation immune function. It is not doubt that Theorem 1 is very important, for it can explain that, there exists certain contact between the correlation immunity and e-derivative \( ef(x) / ex_i \) of H Boolean function \( f(x) \).

Theorem 1 is not a sufficient theorem. We need deeply study the contact between the correlation immunity and e-derivative \( ef(x) / ex_i \) of H Boolean function \( f(x) \).

In Theorem 2, we discuss the compatible condition of \( m \)-order correlation immunity and 1st-order algebraic immunity of H Boolean function with \( w_i(f(x)) = 2^{n-1} + 2^{n-2} \). Namely, discussing the contact of
e-derivative and correlation immunity of this class of H Boolean functions. We obtain the sufficient and necessary condition on the compatibility of \( m \)-order correlation immunity and 1st-order algebraic immunity for this kind of H Boolean functions.

**Theorem 2:** For an H Boolean function \( f(x) \) with \( w_1(f(x)) = 2^{n-1} + 2^{n-2} \) and correlation immunity of order \( m \) \((m \geq 1)\), \( A_I(f) = 1 \) iff there exists affine functions \( \omega_x \) and \( \omega_x \). There are \( w_1(\omega_x) > m \) \((i = 1, 2)\), \( \omega_x = ef(x)/\epsilon_{x} \), \( \omega_x f(x)/dx = f(x)df(x)/dx \), and \( w_1(\omega_x f(x)/\epsilon_{x}) = 2^{n-2} \).

Proof: Firstly, we would prove the necessary condition for the weight of \( \omega \).

If \( A_I(f) = 1 \) and we suppose that \( f(x) \) or \( 1f(x) \) have 1st-degree annihilators \( \omega_x \), there must be \( w_1(\omega_x) > m \).

If \( w_1(\omega_x) \leq m \) , As \( w_1(f(x)) = 2^{n-1} + 2^{n-2} \), there certainly has \( w_1(\omega_x f(x)) = 2^{n-2} + 2^{n-3} \), and also there are \( w_1(\omega_x (1+f(x))) = 2^{n-3} \), which is contradictory with the fact that \( \omega_x \) is annihilators of \( f(x) \) or \( 1f(x) \).

So there must will be \( w_1(\omega_x) > m \).

Thus, if \( \omega_x = ef(x)/\epsilon_{x} \), then \( \omega_x (1+f(x)) = \omega_x + \omega_x f(x) = 0 \), thereby \( A_I(f) = 1 \). If \( \omega_x f(x)/dx = f(x)df(x)/dx \), and \( w_1(\omega_x f(x)/\epsilon_{x}) = 2^{n-2} \),

\[
\omega_x f(x)/dx + \omega_x f(x)/\epsilon_{x} = w_1(\omega_x f(x)/dx) + w_1(\omega_x f(x)/\epsilon_{x}) = 2^{n-1}.
\]

(14)

So known by (14) and \( w_1(\omega_x) = 2^{n-1} \), \( \omega_x \) is a subfunction of \( f(x) \). So we can get \( \omega_x (1+f(x)) = 0 \), and then \( A_I(f) = 1 \).

Conversely, if \( A_I(f(x)) = 1 \), we can suppose that \( \omega_x \) is the annihilator of \( f(x) \) or \( 1f(x) \). Owing to \( w_1(\omega_x) = 2^{n-1} \) and \( w_1(f(x)) = 2^{n-2} + 2^{n-2} \), there is \( \omega_x f(x) \neq 0 \). So it can only be \( \omega_x f(x) = 0 \) and \( \omega_x f(x) = \omega_x \), and then

\[
w_1(\omega_x f(x)/dx) + w_1(\omega_x f(x)/\epsilon_{x}) = 2^{n-1}.
\]

(15)

Obviously, there is

\[
w_1(\omega_x f(x)/dx) + w_1(\omega_x f(x)/\epsilon_{x}) = 2^{n-1}.
\]

(16)

Subtracting (15), we get

\[
w_1(\omega_x f(x)/dx) - w_1(\omega_x f(x)/dx) = 0.
\]

(17)

Solve the equation (17), we can only get the solvability of (17) as following:

1) \( w_1(\omega_x f(x)/dx) = w_1(\omega_x f(x)/dx) = 0 \)

2) \( w_1(\omega_x f(x)/dx) = w_1(\omega_x f(x)/dx) \neq 0 \)

The solution which is equivalent to 1) is \( \omega_x = ef(x)/\epsilon_{x} \), and the solution which is equivalent to formula 2) is \( \omega_x f(x)/dx = f(x)df(x)/dx \) and \( w_1(\omega_x f(x)/\epsilon_{x}) = 2^{n-2} \). The proof ends.

Remark 2: Theorem 2 indicates the necessary and sufficient condition of the compatibility of m-order correlation immunity and 1-order algebraic immunity is the e-derivative \( ef(x)/\epsilon_{x} \) and the derivative part \( f(x)df(x)/dx \) of \( f(x) \) satisfy a certain quantitative relation with affine function \( \omega_x \) \((w_1(\omega_x) > m)\) and \( \omega_x = ef(x)/\epsilon_{x} \). That is, the compatibility between m-order correlation immunity and 1-order algebraic immunity of \( f(x) \) is decided by whether that e-derivative is a linear function or derivative part \( f(x)df(x)/dx \) can form a linear function with the part values of e-derivative. Theorem 2 also shows \( ef(x)/\epsilon_{x} \) is an annihilator of the lowest algebraic degree of \( f(x) \) and \( 1f(x) \).

In Theorem 3, we discuss the relations between m-order correlation immunity and the derivative part \( f(x)df(x)/dx \) of H Boolean function \( f(x) \) with the Hamming weight of \( 2^{n-1} + 2^{n-2} \). We get the sufficient and necessary condition, which were expressed by the derivative part \( f(x)df(x)/dx \) entirely, for this
class of H Boolean functions $f(x)$ with correlation immunity order $m$. Namely, this class of H Boolean functions $f(x)$ with $m$-order correlation immunity decide by the derivative part $f(x)df(x)/dx$ entirely.

**Theorem 3:** If an H Boolean function $f(x)$ with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$ is a correlation immune function of order $m$, iff for $\omega, x \in GF(2)^n (1 \leq w_i(\omega) \leq m)$, we have

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

**Proof:** There is

$$w_i(f(x) + ox) = w_i(f(x)df(x)/dx + ox) + w_i(ef(x)/ex + ox) - w_i(ox) \quad (i = 1, 2, \cdots, n).$$

By the known condition, Theorem 1 and Lemma 2, there are $w_i(f(x) + ox) = 2^{n-1}$, $w_i(ef(x)/ex) = 2^{n-1}$ and $w_i(ef(x)/ex + ox) = 2^{n-1} \quad (i = 1, 2, \cdots, n).$ So by (16), we can get

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

Conversely, when (18) is correct, since $f(x)$ is an H Boolean function, and $w_i(f(x)df(x)/dx) = 2^{n-2}$, then

$$w_i(f(x)df(x)/dx) = w_i(oxf(x)df(x)/dx) + w_i((1 + ox)f(x)df(x)/dx) = 2^{n-2}. \quad (19)$$

Known by (18) and (19), we can get

$$w_i((1 + ox)f(x)df(x)/dx) = 2^{n-3}. \quad (20)$$

As $w_i(f(x)) = 2^{n-1} + 2^{n-2}$ and $w_i(ef(x)/ex) = 2^{n-1}$, there is

$$oxdf(x)/dx + ef(x)/ex = ox. \quad (22)$$

By (21) and (22), we can get

$$w_i(oxef(x)/ex) = 2^{n-2}, \quad \text{and} \quad w_i((1 + ox)ef(x)/ex) = 2^{n-2}. \quad (23)$$

Therefore, by (18), (19) and (23), there is

$$w_i(oxf(x)) = w_i(oxf(x)df(x)/dx) + w_i(oxef(x)/ex) = 2^{n-2} + 2^{n-3}. \quad (24)$$

Known from (24) and Lemma 3, for all $\omega, x \in GF(2)^n, 1 \leq w_i(\omega) \leq m$, there is $w_i(f(x) + ox) = 2^{n-1}$. Therefore, $CI(f(x)) = m$ is gotten. The proof ends.

**Remark 3:** $ox$ in Theorem 2 is different to the one in Theorem 3. $ox$ in Theorem 2 is the lowest algebraic degree annihilator of $1 + f(x)$. But $ox$ in Theorem 3 mustn't to be an annihilator.

Combining Theorem 1&3, we can obtain the following Corollary 1 which is important.

**Corollary 1:** If an H Boolean function $f(x)$ with $w_i(f(x)) = 2^{n-1} + 2^{n-2}$ is a $m$-order ($m \geq 1$) correlation immune function, and $1 + f(x)$ has the 1st annihilator $g$, then $g$ is a 1st function with at least $m + 1$-variable. Conversely, if $1 + f(x)$ has the $m + 1$-variable 1st-annihilator, and $f(x)$ is a correlation immune function, then $CI(f) \leq m$.

**Proof:** Known by Theorem 1&3, since $f(x)$ is a correlation immune function of order $m$, we can get that for any $\omega, x \in GF(2)^n, 1 \leq w_i(\omega) \leq m$, there is $w_i(oxef(x)/ex) = 2^{n-2}$, and $w_i(oxf(x)df(x)/dx) = 2^{n-3}$. According to Lemma 2, there is

$$w_i(oxf(x)) = 2^{n-2} + 2^{n-3}. \quad (25)$$

Owing to $g(1 + f) = 0$, $g$ is a subfunction of $f(x)$. Suppose the variable number of $g$ is less than $\leq m$ or equal to $m$, by the known conditions, we can get $g$ is a 1st function, $g \in ox$. Therefore, there is

$$w_i(g(1 + f)) = w_i(g) - w_i(gf). \quad (26)$$

From (25), (26) and $w_i(g) = 2^{n-1}$, we can get

$$w_i(g(1 + f)) = w_i(g) - w_i(gf) = 2^{n-1} - (2^{n-2} + 2^{n-3}) = 2^{n-3} \neq 0. \quad (27)$$
Since (27) and \( g(l + f) = 0 \) contradict each other, the variable number of \( g \) must be more than \( m \), that is to say, the variable number of \( g \) is at least \( m + 1 \)-variable.

Conversely, suppose \( CI(f) = m + 1 \), namely \( CI(f) > m \). Known from the above results, the variable number of the 1st-annihilator \( g \) is greater than \( m + 1 \), which contradict the known condition that \( 1 + f(x) \) has \( m + 1 \)-variable 1st-annihilator. So there are must be \( CI(f) \leq m \).

The proof ends.

**Remark 4:** Corollary 1 explains that when \( H \) Boolean functions with \( w_i(f(x)) = 2^{n-1} + 2^{n-2} \) are \( m \)-order correlation immunity and have 1st annihilators, the variables of 1-degree annihilators must be greater than \( m \). That is, the quantity of variables which contain in annihilators of the lowest algebraic degree, is restricted, when the propagation of \( f(x) \) is compatible with \( m \)-order correlation immunity and 1-order algebraic immunity.

Theorem 1~3 and Corollary 1 can help us find an \( H \) Boolean function \( f(x) \) with \( w_i(f(x)) = 2^{n-1} + 2^{n-2} \) and the compatibility of propagation, correlation immunity and algebraic immunity in the following Example 1. \( f(x) \) has compatible of \( CI(f) = 3 \) and \( AI(f) = 1 \).

**Example 1:** There is an \( n \)-variable \( (n = 6) \) \( H \) Boolean function \( f(x) \) with \( w_i(f(x)) = 2^{n-1} + 2^{n-2} \) as following:

\[
f(x) = \sum_{i=0}^{n} x_i + x_{n-1} x_{n-2} x_{n-3} + x_{n-4} x_{n-5} + x_{n-6} + \sum_{i=0}^{n-5} x_i + x_{n-6} x_{n-7} + x_{n-5} x_{n-6} + x_{n-4} x_{n-5} x_{n-6}.
\]

We can get \( CI(f) = 3 \), namely \( f(x) \) is a 3-order correlation immune function. Moreover, \( 1 + f(x) \) have annihilators of the lowest algebraic degree \( x_{n-6} + x_{n-4} + x_{n-3} + x_{n-2} \) and \( ef(x) / ex_n = x_{n-5} + x_{n-4} + x_{n-3} + x_{n-2} + x_{n-1} \), which are 1st functions with 4-variable and \( AI(f) = 1 \).

4. **Conclusions**

By this paper, we get there exists regular contact among the e-derivative, the derivative part and the correlation immunity. We also get that the e-derivative of \( H \) Boolean functions \( f(x) \) plays a decisive role for the algebraic immunity of \( H \) Boolean functions \( f(x) \), when the e-derivative of \( H \) Boolean functions \( f(x) \) with \( w_i(f(x)) = 2^{n-1} + 2^{n-2} \) are linear functions. Meanwhile, we similarly deduce that, the e-derivative plays a decisive role for the algebraic immunity order of this class of \( H \) Boolean functions \( f(x) \), when \( \deg(ef(x) / ex_n) \geq 2 \).

The results in this paper show that it is not only an original and effective research method to study cryptographic properties of Boolean functions, but also a new method with which we can deeply reveal the different relationship of cryptographic properties, e-derivative and derivative using e-derivative and derivative as research tools. Overall, the results and methods in this paper have important significance to study cryptographic properties of Boolean functions and to research the security of cryptographic systems.

**Acknowledgement**

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

**References**


