On Relevance of Derivative, E-derivative, and Correlation Immunity of Sum and Product for Boolean Functions

JINGLIAN HUANG and ZHUO WANG

ABSTRACT

In this paper, we discuss the relationship among derivative, e-derivative, and correlation immunity of the sum and the product for Boolean functions. We obtain the sufficient and necessary condition, which the sum of two elastic Boolean functions represented by the derivative and e-derivative are elastic Boolean functions. And we get the sufficient condition, which the sum and product of the correlation immune Boolean functions represented by the derivative are correlation immune. We also get the sufficient and necessary condition of the sum of two functions which is m-order correlation immunity, which is the product of two functions with m-order correlation immunity. At the same time, we obtain the sufficient conditions for correlation immunity of the derivatives and the e-derivatives of the sum of two functions and so on. The correlation immunity of Boolean function is closely related to the derivative and e-derivative of functions.

INTRODUCTION

The correlation immunity of Boolean functions is a necessary property of cryptographic system to resist related attacks. The higher the order of Boolean functions’ correlation immunity is, the stronger the ability of cryptosystems to resist the attacks. But except against the related attacks, the password system also needs to resist the linear attack, differential attack, algebraic attack and other attacks [1]. Except correlation immunity, Boolean functions also have a variety of other good cryptographic properties such as nonlinearity, diffusion, linear complexity, algebraic immunity [2~5] and so on. There tend to have mutual conditionality between these cryptographic properties, for example, between correlation immunity and algebraic there is a mutual restriction relation. Correlation immune order increased, linear complexity will be reduced. Therefore, the study of the relevant immunity is complex, we can not only
consider improving the correlation immunity order, and a wide range of in-depth study should be done [1~5].

In this paper, we study some the relationship and mutual influence, including: the correlation immunity of the sum function and the product function; the correlation immunity of Boolean functions, and the correlation immunity of derivative part and e-derivative; the correlation immunity of the sum functions and product functions, and the correlation immunity of derivative part and e-derivative of product functions and so on, and gives the corresponding results.

PRELIMINARIES

To study cryptographic properties of H Boolean functions, we proposed the concept of the e-derivative. The e-derivative [6~7] and derivative [8] are defined here as Definition 1&2.

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

$$
ef(x) / e(x_{i_1}, x_{i_2}, \ldots, x_{i_r})
= f(x_{i_1}, x_{i_2}, \ldots, x_{i_1}, 1 + x_{i_1}, 1 + x_{i_2}, \ldots, 1 + x_{i_r}, \ldots, x_n)
(1 \leq i_1 \leq n, 1 \leq i_1 \leq i_2 \leq \ldots \leq i_r \leq n, 1 \leq r \leq n)$$

(1)

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.

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

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

$$\partial f(x) / \partial(x_{i_1}, x_{i_2}, \ldots, x_{i_r})
= f(x_{i_1}, x_{i_2}, \ldots, x_{i_1}, x_{i_2}, \ldots, x_{i_r}, x_{i_{r+1}}, \ldots, x_n) + f(x_{i_1}, x_{i_2}, \ldots, 1 + x_{i_1}, 1 + x_{i_2}, \ldots, x_{i_r}, \ldots, x_n)
(1 \leq i_1 \leq n, 1 \leq i_1 \leq i_2 \leq \ldots \leq i_r \leq n, 1 \leq r \leq n)$$

(2)

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

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

**Lemma:** For any arbitrary Boolean function \(f(x)\), the following equations are true:
\[
f(x) = f(x)\frac{df(x)}{dx_i} + ef(x)/ex_i \quad (i = 1, 2, \ldots, n),
\]
and
\[
w_i(f(x)) = w_i(f(x)\frac{df(x)}{dx_i}) + w_i(ef(x)/ex_i) = 2^{i-1} w_i(\frac{df(x)}{dx_i}) + w_i(ef(x)/ex_i)
\quad (i = 1, 2, \ldots, n).
\]

Calling \(f(x)\frac{df(x)}{dx_i}\) is derivative part of \(f(x)\), and \(ef(x)/ex_i\) is e-derivative of \(f(x)\).

**THE CORRELATION IMMUNITY OF BOOLEAN FUNCTIONS, DERIVATIVE AND E-DERIVATIVE**

In Theorem 1, we discuss the derivative and e-derivative conditions which the sum functions of two resilient Boolean functions are still resilient Boolean functions firstly.

**Theorem 1:** Set two resilient Boolean functions \(f_1(x)\) and \(f_2(x)\) \((f_1(x), f_2(x) \in GF(2^{2^n}))\), then \(f_1(x) + f_2(x)\) is a resilient Boolean function iff \(w_i(\omega(x) = 1)\), there are
\[
w_i(f_1(x)f_2(x)/dx_i) + w_i(f_1(x)f_2(x)/dx_i ef_1(x)/ex_i) + w_i(ef_1(x)/ex_i ef_2(x)/ex_i) = 2^{n-2}
\]
\[
w_i(\omega(x)f_1(x)f_2(x)/dx_i) + w_i(\omega(x)f_1(x)f_2(x)/dx_i ef_1(x)/ex_i) + w_i(\omega(x)f_1(x)/ex_i ef_2(x)/ex_i) = 2^{n-2}
\]

**Proof:** 1) By Lemma, there are
\[
w_i(f_1(x) + f_2(x)) = w_i(f_1(x)) + w_i(f_2(x))
-2[w_i(f_1(x)f_2(x)/dx_i) + w_i(f_1(x)f_2(x)/dx_i ef_2(x)/ex_i) + w_i(f_1(x)(f_2(x)/dx_i ef_2(x)/ex_i) + w_i(ef_1(x)/ex_i ef_2(x)/ex_i)].
\]

Since \(f_1(x)\) and \(f_2(x)\) are resilient Boolean functions, known by the above formula \(f_1(x) + f_2(x)\) has the balance iff (3) holds.
2) For \( ax \ (w_i(\omega) = 1) \), because \( f_1(x) \) and \( f_2(x) \) are correlation immune functions, so there have

\[
w_i(f_1(x) + f_2(x) + ax) = w_i(f_1(x) + ax + f_2(x) + ax) = w_i(f_1(x) + ax) + w_i(f_2(x) + ax) - 2w_i(ax) + w_i(axf_1(x)f_2(x)) = 2[2w_i(axf_1(x)f_2(x)) - w_i(f_1(x)f_2(x))] \]  

Due to

\[
w_i(f_1(x)f_2(x)) = w_i(f_1(x)df_1(x)/dx, f_2(x)df_2(x)/dx) + w_i(f_1(x)df_1(x)/dx, ef_2(x)/ex) + w_i(ef_1(x)/ex, ef_2(x)/ex),
\]

Known from (3) and (5), \( f_1(x) + f_2(x) \) are correlation immune functions iff (4) holds.

So, \( f_1(x) + f_2(x) \) are resilient Boolean functions iff (3) and (4) holds.

The proof ends.

By the proof of Theorem 1, Corollary 1 can be obtained as follows.

**Corollary 1:** If \( f_1(x), f_2(x) \in GF(2)^{GF(2^n)} \) are both m-order correlation immune functions, \( f_1(x) + f_2(x) \) are m-order correlation immune functions iff the product of two functions \( f_1(x)f_2(x) \) are m-order correlation immune functions too.

In Theorem 1 and Corollary 1, when \( f_1(x) \) and \( f_2(x) \) are all correlation immunity functions, we reveal the correlation immunity of the sum and the product of two functions. Theorem 2 reveals the sufficient conditions of correlation immunity of the sum functions and product functions of two arbitrary functions represented by the derivative.

**Theorem 2:** For \( f_1(x), f_2(x) \in GF(2)^{GF(2^n)} \), if there are \( \partial f_1(x)/\partial(x_1, x_2, \ldots, x_n) = \partial f_2(x)/\partial(x_1, x_2, \ldots, x_n) = 0 \), \( f_1(x) + f_2(x) \) and \( f_1(x)f_2(x) \) are correlation immune functions.

**Proof:** Denote \( f(x) = f_1(x) + f_2(x) \). Due to \( \partial f(x)/\partial(x_1, x_2, \ldots, x_n) = \partial f_1(x)/\partial(x_1, x_2, \ldots, x_n) = 0 \), So

\[
\partial f(x)/\partial(x_1, x_2, \ldots, x_n) = \partial(f_1(x) + f_2(x))/\partial(x_1, x_2, \ldots, x_n) = \partial f_1(x)/\partial(x_1, x_2, \ldots, x_n) + \partial f_2(x)/\partial(x_1, x_2, \ldots, x_n) = 0.
\]

For \( i = 1, 2, \ldots, n \), there are

\[
w_i(f(x)|x_i = 0) = w_i(f(x)|x_i = 1) = 2^{-i} w_i(f(x)).
\]

So, for any \( x_i \), \( i = 1, 2, \ldots, n \), there are

\[
w_i(f(x) + x_i) = w_i(f(x)) + w_i(x_i) - 2w_i(x_if(x)) = w_i(x_i) = 2^{-i}.
\]

Therefore, \( f(x) = f_1(x) + f_2(x) \) are correlation immune functions.
Known from the Corollary 1 of Theorem 1, \( f_1(x)f_2(x) \) are correlation immune functions too. The proof ends.

The following Theorems 3&4 discuss the relationship of correlation immunity among Boolean functions \( f(x) \), the derivative part \( f(x)df(x)/dx_n \) and the e-derivative \( ef(x)/ex_n \) of \( f(x) \).

**Theorem 3:** For \( f(x) \in GF(2)^{GF(2^r)} \), if \( f(x)df(x)/dx_n \) and \( ef(x)/ex_n \) are \( m \)-order correlation immunity, then \( f(x) \) also \( m \)-order correlation immune functions.

**Proof:** By the Lemma, for \( x \in GF(2) \), there have

\[
\begin{align*}
    w_i(f(x) + o\alpha) &= w_i(f(x)df(x)/dx_n + o\alpha + ef(x)/ex_n + o\alpha) \\
    &= w_i(f(x)df(x)/dx_n + o\alpha + ef(x)/ex_n + o\alpha) + w_i(o\alpha) - 2w_i(o\alpha(f(x)df(x)/dx_n + ef(x)/ex_n)) \\
    &= w_i(f(x)df(x)/dx_n + o\alpha) + w_i(ef(x)/ex_n + o\alpha) - 2w_i(o\alpha f(x)df(x)/dx_n).
\end{align*}
\]

So, if \( w_i(f(x)df(x)/dx_n + o\alpha) = 2^{n-1} \), and \( w_i(ef(x)/ex_n + o\alpha) = 2^{n-1} \), that is, when \( f(x)df(x)/dx_n \) and \( ef(x)/ex_n \) are \( m \)-order correlation immunity, \( f(x) \) are \( m \)-order correlation immune functions. The proof ends.

Theorem 3 is a sufficient condition theorem for \( f(x) \) \( m \)-order correlation immunity, not a necessary condition. And Theorem 4 reveals that if \( f(x) \) is correlation immunity, also \( f(x)df(x)/dx_n \) and \( ef(x)/ex_n \) must be correlation immunity.

**Theorem 4:** For \( f(x) \in GF(2)^{GF(2^r)} \), if there are \( \partial f(x)/\partial(x_i,x_2,\ldots,x_n) = 0 \), then \( f(x)df(x)/dx_n \) and \( ef(x)/ex_n \) are correlation immune functions, and

\[
\partial(f(x)df(x)/dx_n)/\partial(x_i,x_2,\ldots,x_n) = 0, \quad \partial(ef(x)/ex_n)/\partial(x_i,x_2,\ldots,x_n) = 0.
\]

**Proof:** Due to \( \partial f(x)/\partial(x_i,x_2,\ldots,x_n) = 0 \), there are

\[
[f(x)df(x)/dx_n + ef(x)/ex_n]_{x_i=1} + [f(x)df(x)/dx_n + ef(x)/ex_n]_{x_i=0} = 0.
\]

So there are

\[
\begin{align*}
    w_i(f(x)df(x)/dx_n | x_i = 0) &= w_i(f(x)df(x)/dx_n | x_i = 1) = 2^{-1} w_i(f(x)df(x)/dx_n) \\
    w_i(ef(x)/ex_n | x_i = 0) &= w_i(ef(x)/ex_n | x_i = 1) = 2^{-1} w_i(ef(x)/ex_n).
\end{align*}
\]

Known from the same proof of Theorem 2, \( f(x)df(x)/dx_n \) and \( ef(x)/ex_n \) are both correlation immune functions.
Known by Lemma, there are
\[ \partial f(x) / \partial (x_1, x_2, \ldots, x_n) \]
\[ = \partial (f(x) df(x)/dx_n)/\partial (x_1, x_2, \ldots, x_n) + \partial (ef(x)/ex_n)/\partial (x_1, x_2, \ldots, x_n). \]
\[ = 0 \]
Also, because of \( df(x)/dx_n ef(x)/ex_n = 0 \), so there must be
\[ \partial (f(x) df(x)/dx_n)/\partial (x_1, x_2, \ldots, x_n) = 0, \partial (ef(x)/ex_n)/\partial (x_1, x_2, \ldots, x_n) = 0. \]

The proof ends.

The following Theorem 5&6 discuss the impact of correlation immunity of derivative part and e-derivative part of the product of two Boolean functions on correlation immunity of the sum and product of two Boolean functions.

**Theorem 5:** For \( f_1(x), f_2(x) \in GF(2)^{GF(2)^n} \), if \( f_1(x) \) and \( f_2(x) \) are \( m \)-order correlation immune functions, and \( ef_1(x)/ex_n ef_2(x)/ex_n \) and \( f_1(x)df_1(x)/dx_n f_2(x)df_2(x)/dx_n + f_1(x)df_1(x)/dx_n ef_2(x)/ex_n + f_2(x)df_2(x)/dx_n ef_1(x)/ex_n \) are \( m \)-order correlation immune functions, then \( f_1(x)df_1(x)/dx_n f_2(x)df_2(x)/dx_n + f_1(x)df_1(x)/dx_n ef_2(x)/ex_n + f_2(x)df_2(x)/dx_n ef_1(x)/ex_n \) are \( m \)-order correlation immune functions.

**Proof:** Known by Lemma, there are
\[ f_1(x)df_1(x)/dx_n f_2(x)df_2(x)/dx_n + f_1(x)df_1(x)/dx_n ef_2(x)/ex_n + f_2(x)df_2(x)/dx_n ef_1(x)/ex_n \]
\[ = f_1(x)df_1(x)/dx_n f_2(x)df_2(x)/dx_n + f_1(x)df_1(x)/dx_n ef_2(x)/ex_n + \]
\[ + f_2(x)df_2(x)/dx_n ef_1(x)/ex_n. \quad (6) \]

To record (6) as \( f_1(x)df_1(x)/dx_n f_2(x)df_2(x)/dx_n + f_1(x)df_1(x)/dx_n ef_2(x)/ex_n + f_2(x)df_2(x)/dx_n ef_1(x)/ex_n \). Then we can get
\[ h(x) \cdot ef_1(x)/ex_n ef_2(x)/ex_n = 0. \]
So for any \( \omega x (1 \leq \omega \leq m) \), we can deduce
\[ w_1(f_1(x)df_1(x)/dx_n f_2(x)df_2(x)/dx_n + f_1(x)df_1(x)/dx_n ef_2(x)/ex_n + \omega x) = w_1(h(x) + \omega x) + w_1(ef_1(x)/ex_n ef_2(x)/ex_n + \omega x) - w_1(\omega x). \]

Shows that, when
\[ h(x) = f_1(x)df_1(x)/dx_n f_2(x)df_2(x)/dx_n + f_1(x)df_1(x)/dx_n ef_2(x)/ex_n + f_2(x)df_2(x)/dx_n ef_1(x)/ex_n \]
\[ = f_1(x)df_1(x)/dx_n f_2(x)df_2(x)/dx_n + f_1(x)df_1(x)/dx_n ef_2(x)/ex_n + f_2(x)df_2(x)/dx_n ef_1(x)/ex_n \]
\[ \quad (7) \]
\( h(x) \) are \( m \)-order correlation immune functions, and \( ef_1(x)/ex_n ef_2(x)/ex_n \) are \( m \)-order correlation immune functions, \( f_1(x)df_2(x)/dx_n \) and \( f_2(x)df_2(x)/dx_n \) are \( m \)-order correlation immune functions.

Thus, known from the Corollary 1 of Theorem 1, \( f_1(x) + f_2(x) \) are \( m \)-order correlation immune functions. The proof ends.

**Theorem 6:** If \( f_1(x), f_2(x) \in GF(2)^{GF(2)^n} \), there are
\[ \frac{\partial f_1(x)}{\partial (x_1, x_2, \ldots, x_n)} = \frac{\partial f_2(x)}{\partial (x_1, x_2, \ldots, x_n)} = 0. \]
then $h(x)$ in (7), and $e_f(x)/e_x ef_z(x)/e_x$ are $m$-order correlation immune functions.

**Proof:** Due to

\[
(d_f(x)/dx, df_z(x)/dx_n, f_1(x)/df_1(x)/dx_n ef_z(x)/e_x) = 0,
\]
\[
(d_f(x)/dx, df_z(x)/dx_n, f_2(x)/df_2(x)/dx_n ef_f(x)/e_x) = 0,
\]
\[
(f_1(x)/df_1(x)/dx_n, ef_z(x)/e_x) = 0,
\]
\[
(f_2(x)/df_2(x)/dx_n, ef_f(x)/e_x) = 0.
\]

And

\[
d(f_i(x)/dx_n f_1(x)/df_z(x)/dx_n + f_i(x)/df_1(x)/dx_n + df_i(x)/dx_n df_z(x)/dx_n, \\
\quad df_i(x)/dx_n df_z(x)/dx_n, \\
\quad (ef_f(x)/e_x, ef_z(x)/e_x) = 0,
\]
\[
e(ef_f(x)/e_x, ef_z(x)/e_x) = ef_f(x)/e_x ef_z(x)/e_x ≠ 0.
\]

So (7) are derivative part of $f_i(x)f_z(x)$. And $e_f(x)/e_x ef_z(x)/e_x$ are e-derivative of $f_i(x)f_z(x)$.

Known by Theorem 4 and the conditions of Theorem 6, $h(x)$ and $e_f(x)/e_x ef_z(x)/e_x$ are correlation immune functions. The proof ends.

By the proof of Theorem 6, we can get Corollary 2 and Corollary 3.

**Corollary 2:** The e-derivative of the product of two Boolean functions $f_i(x)f_z(x)$ is the product of e-derivative of two Boolean functions $f_i(x)$ and $f_z(x)$. The derivative part of the product of two Boolean functions $f_i(x)f_z(x)$ is $h(x)$, i.e. (7).

**Corollary 3:** If $f_i(x)$ and $f_z(x)$ are correlation immune functions, then $f_i(x)f_z(x)$ and $f_i(x) + f_z(x)$ are correlation immune functions iff $h(x)$ and $e_f(x)/e_x ef_z(x)/e_x$ are correlation immune functions.

**CONCLUSIONS**

Through in-depth discussion, the results obtained in this paper show that the relationship between the correlation immunity and the internal value structure of the function is closely related. Therefore, we can find and construct Boolean functions with higher order correlation immunity, and study the correlation between the correlation immunity of Boolean function and other cryptographic properties by the derivative and e-derivative of Boolean function.
ACKNOWLEDGEMENT

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

REFERENCES