On extended algebraic immunity

Gaofei Wu*, Yuqing Zhang†and Weiguo Zhang‡

Abstract

In this paper, two sufficient conditions for a Boolean function with optimal extended algebraic immunity are given. It is shown that almost all the known functions possess maximum possible algebraic immunity. The results show that about half of them do not possess optimal extended algebraic immunity.

Keywords: Stream ciphers, Boolean functions, Extended algebraic immunity, Algebraic immunity.

1 Introduction

Recently, algebraic attacks have received lots of attention in the cryptographic literature. It is known that Boolean functions should have good cryptographic properties to resist the new attacks. Until now, there are several constructions of boolean functions with optimal algebraic immunity (AI) (for example, see [1], [2], [4], [5], [8], [9], [10], [12]). In [14], Xian-Mo Zhang et al. extended the concept of algebraic immunity. They argued that a function f may be replaced by another Boolean function f^c, called the algebraic complement of f, and defined extended algebraic immunity (EAI). They proved that $AI(f) - EAI(f) \leq 1$, and showed that $AI(f) - EAI(f) = 1$ holds for a large number of cases. This is also demonstrated in this paper. The relations between different properties of a Boolean function f and its algebraic complement f^c were studied in [11], and they argued that a necessary condition for an n-variable Boolean function to achieve the maximum possible EAI is that n should be even. Because a difference of only 1 between the algebraic immunities of two functions can make a crucial difference with respect to algebraic attacks, it is necessary to analyze extended algebraic immunity.

In this paper, two sufficient conditions for a Boolean function of an even number variables with optimal EAI are given. Then we study almost all the known functions possess maximum possible algebraic immunity for their EAI. The results show that about half of them do not have optimal EAI.

The rest of the paper is organized as follows. In Section 2, the basic concepts and notions are presented. Two theorems about sufficient conditions for a Boolean function with optimal EAI are given in Section 3, and using them we analyze the EAI of some known functions with maximum AI. In Section 4, some further results and proofs about Boolean functions with optimal EAI are given. Finally, Section 5 concludes the correspondence.

*The author is with the Key Lab of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China. Email: 471214507@qq.com.

†The author is with the National Computer Network Intrusion Protection Center, GUCAS, Beijing 100043, China.

‡Corresponding address: ISN Lab, Xidian University, Xi'an 710071, P.R.China.

2 Preliminary

A Boolean function $f(x)$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$. Let $\mathbb{B}_n$ denote the set of all n-variable Boolean functions. The basic representation of a Boolean function $f(x_1, x_2, \cdots, x_n)$ is by the output column of its truth table, i.e., a binary string of length 2^n,

$$f = [f(0, 0, \cdots, 0), f(1, 0, \cdots, 0), \cdots, f(1, 1, \cdots, 1)].$$

$f(x)$ is generally represented by its algebraic normal form (ANF):

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u (\prod_{i=1}^{n} x_i^{u_i}) \tag{1}$$

where $\lambda_u \in \mathbb{F}_2$, $u = (u_1, u_2, \cdots, u_n)$. $\prod_{i=1}^{n} x_i^{u_i}$ is called a term in ANF of f. It is well known that $\lambda_u = \sum_{x \preceq u} f(x)$, where $x \preceq u$ means that u covers x, that is, if $x = (x_1, x_2, \cdots, x_n), u = (u_1, u_2, \cdots, u_n)$, satisfies the condition that $u_i = 1$ wherever $x_i = 1$. The algebraic degree of $f(x)$, denoted by $deg(f)$, is the maximal value of $wt(u)$ such that $\lambda_u \neq 0$, where $wt(u)$ denotes the Hamming weight of u. Let $supp(f) = \{x | f(x) = 1, x \in \mathbb{F}_2^n\}$, the Hamming weight of f, denote by $wt(f)$, is the cardinality of the support $supp(f)$. A Boolean function f is said to be balanced if $wt(f) = 2^{n-1}$.

Definition 1: For $f \in \mathbb{B}_n$, define $AN(f) = \{g \in \mathbb{B}_n | f * g = 0\}$. Any function $g \in AN(f)$ is called an annihilator of f. The algebraic immunity (AI) of f is the minimum degree of all the nonzero annihilators of f or $f + 1$, and we denote it by $AI(f)$.

Definition 2: Let $\triangle(x) = (1 + x_1)(1 + x_2) \cdots (1 + x_n)$, where $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$. Define $f^c(x) = f(x) + \triangle(x)$, $f^c(x)$ is called the algebraic complement of $f(x)$, i.e., $f^c(x)$ contains all monomials that are not in the ANF of $f(x)$.

It is easy to see that $(f^c)^c(x) = f(x)$, $f^c(x) + 1 = (f(x) + 1)^c$, $\forall f(x) \in \mathbb{B}_n$. From the definition of $\triangle(x)$, it is trivial to prove the following:

1. $f^c(x) = f(x)$ if $x \neq 0$, and $f^c(0) = f(0) + 1$.
2. $\triangle(x) \neq 0$ iff (if and only if) $x = 0$.
3. $f(x) \triangle (x) = 0$ if $f(0) = 0$, $f(x) \triangle (x) = \triangle(x)$ if $f(0) = 1$.

Definition 3: The extended algebraic immunity $EAI(f)$ is defined as follows: $EAI(f) = min\{deg(g) | g \in AN(f) \bigcup AN(f+1) \bigcup AN(f^c) \bigcup AN(f^c+1)\}$. i.e., $EAI(f) = min\{AI(f), AI(f^c)\}$.

Lemma 1[14]: Let $f \in \mathbb{B}_n$, then (1) $AI(f) - EAI(f) = 0$ or 1, (2) $|AI(f) - AI(f^c)| = 0$ or 1.

Definition 4: Let f is a Boolean functions with n variables. We called f $0 - CM$ $(1 - CM)$ if $f(0) = 0 (f(0) = 1)$.

Lemma 2[3]: Let $f \in \mathbb{B}_n$, then there is a nonzero Boolean function $g \in \mathbb{B}_n$ of degree at most $\lceil n/2 \rceil$, such that $deg(f * g) \leq \lceil n/2 \rceil$.

From Lemma 2, it is known that upper bound of AI and EAI is $\lceil n/2 \rceil$.

Lemma 3[11]: Let $f \in \mathbb{B}_n$, if n is odd, then $EAI(f) \leq \lceil n/2 \rceil - 1$. Further if $AI(f) = \lceil n/2 \rceil$, Then $EAI(f) = \lceil n/2 \rceil - 1$.

It is well known that a function of odd variables with maximum algebraic immunity must be balanced, but while f is balanced, f^c is unbalanced. Moreover Lemma 3 shows that a Boolean function of an odd number variables can't have optimal EAI.

Lemma 4[11]: Let $f \in \mathbb{B}_n$, and n is even, if $AI(f) = n/2$. Then:

1. If f is $0 - CM$, and $wt(f) = \sum_{i=0}^{n/2} \binom{n}{k}$, then $EAI(f) = n/2 - 1$.
2. If f is $1 - CM$, and $wt(f) = \sum_{i=0}^{n/2-1} \binom{n}{k}$, then $EAI(f) = n/2 - 1$.

3 Two sufficient conditions for Boolean functions with optimal extended algebraic immunity

There are two main classes of Boolean functions achieving optimal algebraic immunity (see [1], [2], [4]).In this section, their extended algebraic immunity are studied. The construction in [4] is as follows. Let $f \in \mathbb{B}_n$, and $n = 2k$, then

$$f(x) = \begin{cases} 0, wt(x) < n/2; \\ 1, wt(x) > n/2; \\ g(x), \text{wt(x)=n/2}. \end{cases}$$

Where $g(x)$, $x \in \{x | wt(x) = n/2\}$, is a random Boolean function.

Theorem 1: Let $f(x) \in \mathbb{B}_n$ is a function given above, if $g(x) \not\equiv 1, \forall x \in \{x | wt(x) = n/2\}$, then $EAI(f) = k = n/2$.

Proof: $supp(f) = \{x | wt(x) > n/2\} \bigcup \{x | wt(x) = n/2, g(x) = 1\}$, $supp(f^c) = \{x | wt(x) > n/2\} \bigcup \{x | wt(x) = n/2, g(x) = 1\} \bigcup \{0\}$, $supp(f) \subseteq supp(f^c)$, then $AN(f) \supseteq AN(f^c)$, since f has maximum algebraic immunity, f^c doesn't have annihilator of degree $< n/2$. Now we consider $f^c + 1$, suppose $h(x)$ is an annihilator of $f^c + 1$, and $deg(h) < n/2$, one needs to show that $g(x) = 0$. From $h(x) = 0, \forall x \in supp(f^c + 1)$ and $supp(f^c + 1) = \{x | wt(x) < n/2\} \backslash \{0\} \bigcup \{x | g(x) = 0, wt(x) = n/2\}$, considering the degree of functions in $AN(f^c + 1)$, $h(x)$ was divided into two classes: $h(0) = 0$ and $h(0) = 1$.

In the case $h(0) = 0$, then $h(x) = 0, \forall x \in \{x | wt(x) < n/2\}$. Because $deg(h) < n/2$, $h(x) \equiv 0$; In the case $h(0) = 1$, the function $h(x)$ can be represented as follows:

$$h(x) = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{i<j} a_{ij} x_i x_j + \cdots + a_{k+2,\cdots,n} x_{k+2} \cdots x_n \tag{2}$$

From the preliminary we know that $a_0 = h(0) = 1$, $a_i = h(0) + h(1_i)$, where 1_i denotes the vector that only the i-th bit is 1, others are 0. Because $wt(1_i) = 1$, then $h(1_i) = 0$, and $a_i = 1, \forall 1 \leq i \leq n$. Similarly, one can conclude that $a_{ij} = 1, a_{ijk} = 0, \cdots, a_{k+2,\cdots,n} = 1$, in other words,

$$h(x) = 1 + \sum_{i=1}^{n} x_i + \sum_{i<j} x_i x_j + \cdots + x_{k+2} \cdots x_n \tag{3}$$

However, because $g(x) \not\equiv 1$, suppose $g(z) = 0, \forall z \in \{z | wt(z) = k\}$, then $f^c(z) + 1 = 1$, $h(z) = 0$. Since $wt(z) = n/2$, without lose of generality, suppose the $i_1, i_2, \cdots, i_k$-th bits are 1, and others are 0. $h(z) = 1 + \binom{k}{1} + \binom{k}{2} + \binom{k}{3} + \cdots + \binom{k}{k-1} = 2^k - 1 = 1 mod 2$, this is a contradiction.

To sum up, $f^c(x) + 1$ doesn't have any annihilator with degree $< n/2$, i.e., $AI(f^c) = n/2$, $EAI(f) = n/2$. This completes the proof. □

Remark: It was proved in [11] that if $g(x) \equiv 1, \forall x \in \{x | wt(x) = n/2\}$, then $EAI(f) = k - 1$. Theorem 1 shows that this is the only case such that $EAI(f) = k - 1$.

According to Theorem 1, when $g(x) \equiv 0$, $f(x)$ has maximum EAI. However, it is symmetric, present therefore a risk if attacks using this peculiarity can be found in the future. Moreover, the function f^r doesn't have optimal EAI, where $f^r(x_1, x_2, \cdots, x_n) = f(x_1 + 1, x_2 + 1, \cdots, x_n + 1)$. This is simple to be proved using Lemma 4. Then the following corollary is obtained.

Corollary 1: The extended algebraic immunity is not an invariant under affine transformations.

Using theorem 1, it is easy to see that construction 3 in [5] has optimal EAI: Let $\beta \in \mathbb{B}_n$, $n = 2k$, then

$$\beta(x) = \begin{cases} 1, wt(x) < n/2; \\ 0, wt(x) > n/2; \\ a(x), wt(x) = n/2. \end{cases}$$

Where $a(x)$ is a random Boolean function with the property $a(x) = a(\bar{x}), x \in \{x | wt(x) = k\}$, $\bar{x}$ is the bitwise complement of the vector x, and all the $a(x)$ are not same, i.e., $\beta(x)$ is non-symmetric. Because $a(x) \not\equiv 0$, according to theorem 1, $\beta(x)$ has the maximum EAI. And From Theorem 8 in [5], $\beta(x)$ also has good resistance against fast algebraic attack.

Recently, based on the univariate polynomial representation of Boolean functions, some functions with optimal AI were proposed (for example, see [2], [9]). Every function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be unique represented as a polynomials $\sum_{i=0}^{i=2^n-1} a_i x^i$, where $a_i \in \mathbb{F}_{2^n}$, f is a Boolean function if and only if $f(x) = (f(x))^2$.

Theorem 2: Let $\alpha(x) \in \mathbb{B}_n$, $n = 2k$, α is a primitive element of the field $\mathbb{F}_{2^n}$, $D = \sum_{i=0}^{i=k-1} \binom{n}{i}$. We have

1. If $supp(\alpha(x)) \supseteq \{\alpha^i, \alpha^{i+1}, \cdots, \alpha^{i+D-1}\}$, and $supp(\alpha(x) + 1) \supseteq \{\alpha^j, \alpha^{j+1}, \cdots, \alpha^{j+D-1}\}$, then the function $\alpha(x)$ has the maximum EAI.
2. If $supp(\alpha(x)) = \{0, \alpha^i, \alpha^{i+1}, \cdots, \alpha^{i+D-2}\}$, and $supp(\alpha(x) + 1) \supseteq \{\alpha^j, \alpha^{j+1}, \cdots, \alpha^{j+D-1}\}$, then $AI(\alpha(x)) = k = n/2$, $EAI(\alpha(x)) = k - 1$.

3. If $supp(\alpha(x)) \supseteq \{\alpha^i, \alpha^{i+1}, \cdots, \alpha^{i+D-2}, \alpha^b\}$. Let $\gamma 1 = (1, \alpha^b, \alpha^{2b}, \alpha^{3b}, \cdots, \alpha^{b(D-1)})$ can't be linear expressed by the first $D-1$ rows of B, which is given later. And $supp(\alpha(x)+1) \supseteq \{\alpha^j, \alpha^{j+1}, \cdots, \alpha^{j+D-2}, \alpha^c\}$, $\gamma 2 = (1, \alpha^c, \alpha^{2c}, \alpha^{3c}, \cdots, \alpha^{c(D-1)})$ can't be linear expressed by the first $D-1$ rows of C, which is given later, then $\alpha(x)$ has maximum EAI.

Proof: First we prove item 1. The proof of $\alpha(x)$ has optimal AI can be found in [2] and [12]. We copy the proof for the readers' convenience. Suppose $g(x) \in \mathbb{B}_n$ is an annihilator of $\alpha(x)$, and $deg(g) < k$, $g(x)$ can be represented as

$$g(x) = \sum_{i=0}^{i=2^n-1} a_i x^i, a_i = 0, \forall wt_2(i) \geq k,$$

where $wt_2(i)$ equals the number of 1's in the binary expansion of i. Without lose of generality, suppose $a_i \neq 0$ if and only if $i \in \{i_1, i_2, \cdots, i_m\}$, where $m \leq D$. Then $g(x) = 0, \forall x \in \{\alpha^i, \alpha^{i+1}, \cdots, \alpha^{i+D-1}\}$. i.e., $B * \gamma = 0$, where $\gamma = (a_{i_1}, a_{i_2}, \cdots, a_{i_m})$, and the matrix B is:

$$B = \begin{pmatrix} \alpha^{ii_1} & \alpha^{ii_2} & \cdots & \alpha^{ii_m} \\ \alpha^{(i+1)i_1} & \alpha^{(i+1)i_2} & \cdots & \alpha^{(i+1)i_m} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha^{(i+D-1)i_1} & \alpha^{(i+D-1)i_2} & \cdots & \alpha^{(i+D-1)i_m} \end{pmatrix}.$$

Let $B' = B(1, 2, \cdots, m)$, where $B(1, 2, \cdots, m)$ denotes the first m rows of B. It is evident that B' is a Vandermonde matrix, $det(B') \neq 0$, then $a_i = 0$ for every $i \in \{i_1, i_2, \cdots, i_m\}$ and $g(x) = 0$. In the same way, it can be seen that there doesn't exist a nonzero annihilator of $\alpha(x)+1$, and to sum up, $AI(\alpha(x)) = k = n/2$. $\alpha(x)$ has optimal EAI is trivial because $supp(\alpha^c(x)) \supseteq \{\alpha^i, \alpha^{i+1}, \cdots, \alpha^{i+D-1}\}$, and $supp(\alpha^c(x)+1) \supseteq \{\alpha^j, \alpha^{j+1}, \cdots, \alpha^{j+D-1}\}$.

Now the proof of item 2 is as follows. Suppose $g(x) \in \mathbb{B}_n$ is an annihilator of $\alpha(x)$ with $deg(g) < k$. The number of terms in ANF of $g(x) \leq D-1$, this is because $g_0 = g(0) = 0$, so using item 1, it can be can seen that $\alpha(x)$ has optimal AI. Since $supp(\alpha^c(x)) = \{\alpha^i, \alpha^{i+1}, \cdots, \alpha^{i+D-2}\}$, there are $D-1$ equations and D variables, there must be a nonzero solution in the system of multivariate algebraic equations. One can simply see that there is only one nonzero solution $a = (a_0, a_2, \cdots, a_{D-1}, a_D, a_{D+1}, \cdots, a_{2^n-1}) = (1, 1, \cdots, 1, 0, 0, \cdots, 0)$, in other words,

$$g(x) = \sum_{\substack{i=0 \\ wt_2(i) < k}}^{i=2^n-1} x^i \tag{4}$$

And so $AI(\alpha^c(x)) < k$, using Lemma 1, the result can be obtained.

Now we prove item 3. $\gamma 1$ can't be linear expressed by the first $D-1$ rows of B, then replaced the last row of B by $\gamma 1$ one will get a matrix $B1$ and $det(B1) \neq 0$, similar to the proof of item 1, $\alpha^c(x)$ and $\alpha(x)$ has no annihilator of degree $< k$. Using the matrix C ($i_1 = 0, i_2 = 1, \cdots, i_m = D-1$) as follows, it is easy to see that $\alpha^c(x)+1$ and $\alpha(x)+1$ has no annihilator of degree $< k$.

$$C = \begin{pmatrix} \alpha^{ji_1} & \alpha^{ji_2} & \cdots & \alpha^{ji_m} \\ \alpha^{(j+1)i_1} & \alpha^{(j+1)i_2} & \cdots & \alpha^{(j+1)i_m} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha^{(j+D-2)i_1} & \alpha^{(j+D-2)i_2} & \cdots & \alpha^{(j+D-2)i_m} \\ \alpha^{ci_1} & \alpha^{ci_2} & \cdots & \alpha^{ci_m} \end{pmatrix}.$$

This completes the proof. □

Using the item 1 of Theorem 2, the functions dl_n constructed in section VI in [9] have maximum EAI, this is because

$$supp(dl_n) = \{\alpha^{2^{n-1}-1}, \cdots, \alpha^{2^n-D-2}\} \bigcup \{1, \alpha, \alpha^2, ..., \alpha^{D-1}\},$$

and

$$supp(dl_n) \supseteq \{1, \alpha, \alpha^2, ..., \alpha^{D-1}\}.$$

And from Theorem 10 in [9] dl_n also has good resistance against fast algebraic attack.

In [10], the authors proposed a combinatorial conjecture about binary strings, and use this conjecture constructed two classes of Boolean functions with optimal algebraic immunity. The construction is as follows:

Construction 1[10]: let $n = 2k$ and α is a primitive element of $\mathbb{F}_{2^k}$. Define function $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$, and $supp(g) = \{\alpha^0, \alpha^1, \cdots, \alpha^{2^{k-1}-1}\}$. Let $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, be defined as $f(x, y) = g(xy^{2^k-2})$.

Similar to the proof of item 1 of Theorem 2, it is easy to see that $f(x, y)$ has maximum extended algebraic immunity.

According to Theorem 2, it is easy to prove the following corollary, which is inspired by [12]:

Corollary 2: Let $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + 1$, be a primitive polynomial over the field $\mathbb{F}_2$, and the companion matrix A of it is

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & c_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}.$$

Define a function $f(x) \in \mathbb{B}_n$, whose support contains $\{A^ib_1, A^{i+1}b_1, \cdots, A^{i+D-1}b_1, \}$, and the support of $f(x) + 1$ contains $\{A^jb_1, A^{j+1}b_1, \cdots, A^{j+D-1}b_1\}$, where $n = 2k, D = \sum_{i=0}^{i=k-1} \binom{n}{i}, 0 \neq b_1 \in \mathbb{F}_2^n$. Then $f(x)$ has maximum EAI.

From Corollary 2, one can conclude that the construction 1 and 2 in [12] have maximum EAI, this is simply because the support of their functions satisfy $supp(f) \supseteq \{b_1, A^1b_1, \cdots, A^{D-1}b_1\}$ and $supp(f + 1) \supseteq \{A^{2^{n-1}+1}b_1, A^{2^{n-1}+2}b_1, \cdots, A^{2^{n-1}+D}b_1\}$.

4 Further results and proofs

In this section, we study some known functions with maximum AI for their EAI. Symmetric Boolean functions are an interesting class of Boolean functions. Denote the set of symmetric Boolean functions by $\mathbb{SB}_n$. A symmetric function can be characterized by a vector

$$v_f = (v_f(0), v_f(1), \cdots, v_f(n)) \in \mathbb{F}_2^{n+1},$$

where $v_f(i) = f(x), \forall x$ with $wt(x) = i$. It is proved in [7] that for odd $n \geq 3$, only the majority function has maximum algebraic immunity. For n is even, in [1] and [8], the authors construct some

classes of symmetric Boolean functions of even variables with maximum algebraic immunity. The constructions are as follows:

Construction 2[1][8]: Let $n = 2k \geq 4$ and $f \in \mathbb{SB}_n$. Let $s_{k-i} = e_{k-i} + e_{k+i}$, where e_j is a vector in $\mathbb{F}_2^n$, such that its j-th position is 1 and the other positions are 0. Then the following functions f has maximum algebraic immunity:

1. $v_f = (\overbrace{11\cdots1}^{k} a \overbrace{00\cdots0}^{k}), a \in \mathbb{F}_2$.
2. $v_f = (\overbrace{11\cdots1}^{k} \overbrace{00\cdots0}^{k} 1)$.
3. $2^i \leq k \leq 3\cdot 2^i - 1, i \geq 0, v_f = (\overbrace{11\cdots1}^{k} b \overbrace{00\cdots0}^{k}) + s_{k-2^i} (b \in \mathbb{F}_2)$.
4. $v_f = (\overbrace{11\cdots1}^{k+1} \overbrace{00\cdots0}^{k}) + s_0, \binom{2k}{k} \equiv 2 mod 4$.
5. $l \geq 1, k = 2^l \cdot s + i, s \geq 0, 1 \leq i \leq 2^l - 1. v_f = (\overbrace{11\cdots1}^{k} \overbrace{00\cdots0}^{k+1}) + e_{2k-i}$.
6. $4\cdot 2^s \leq k < 5 \cdot 2^s, v_f = (\overbrace{11\cdots1}^{k} a \overbrace{00\cdots0}^{k}) + s_{k-3\cdot 2^s} + s_{k-2^s}. a \in \mathbb{F}_2$.

Their EAI are analyzed as follows:

1. - $a = 0$, then f is $1-CM$, and $wt(f) = \sum_{i=0}^{k-1} \binom{n}{i}$, from Lemma 4 and Lemma 1, $EAI(f) = k-1$;
   - $a = 1$, Using Theorem 1, $EAI(f) = k$, however, it is easy to see that $EAI(f^r) = k-1$, which is not the maximum. In an algebraic attack, adversaries are going to compute both $EAI(f)$ and $EAI(f^r)$, they can apply the annihilators whose degree is lowest.
2. According to the proof of Theorem 1, to make sure f has maximum EAI, the following condition should be satisfied: $\sum_{i=0}^{k-1} \binom{n}{i} \equiv 1 mod 2$. This is equivalent to $k = 2^l, l \geq 0$. This shows that $EAI(f) = k-1$ holds for a large number of cases.
3. - $b = 0, k \neq 2^i$, then f is $1-CM$, and $wt(f) = \sum_{i=0}^{k-1} \binom{n}{i}$, from Lemma 4, $EAI(f) = k-1$;
   - $b = 0, k = 2^i$, since $v_{f^c} = (\overbrace{11\cdots1}^{k} \overbrace{00\cdots0}^{k} 1)$, so $AI(f^c) = k$ from item 2, and $EAI(f) = k$. From Lemma 4, $EAI(f^r) = k-1$;
   - $b = 1, k = 2^i$, consider the weight of f and $f(0) = 0$, $EAI(f) = k-1$;
   - $b = 1, k \neq 2^i$, we leave it as an open problem, but from some simple examples, we conjecture that $EAI(f) = k-1$ holds for a large number of cases.
4. Consider the weight of f and $f(0) = 0$, $EAI(f) = k-1$.

5. According to Theorem 1, f has maximum EAI iff $\sum_{j=0}^{k-1}\binom{n-i}{j} \equiv 1 mod 2$. For example, if $i=1$, then $\sum_{j=0}^{k-1}\binom{n-i}{j} = 2^{n-2} = 0 mod 2$, $EAI(f) = k-1$; if $i=2$, f has maximum extended algebraic immunity iff $n = 2^l + 2, \forall l \geq 0$. This means that $EAI(f) = k-1$ holds for a large number of cases.

6.
   - $a = 0$, then f is $1-CM$, and $wt(f) = \sum_{i=0}^{k-1}\binom{n}{i}$, from Lemma 4, $EAI(f) = k-1$;
   - $a = 1$, form a general conclusion seemed to be difficult. But from some simple examples, we conjecture that $EAI(f) = k-1$ holds for a large number of cases.

From the analyze above, it can be concluded that many of symmetric Boolean functions don't have optimal EAI.

In [6], the authors proposed a class of balanced Boolean functions with maximum algebraic immunity. Let $n = 2k, Y_1 = (y_0^1, y_1^1, y_2^1, \cdots, y_{n-1}^1)$,$Y_2 = (y_0^2, y_1^2, y_2^2, \cdots, y_{n-1}^2)$, $Y_1 < Y_2$ means that $\sum_{i=0}^{n-1} y_i^1 2^i < \sum_{i=0}^{n-1} y_i^2 2^i$, $[Y_1, Y_2) = \{y \in \mathbb{F}_2^n | Y_1 \leq Y < Y_2\}$, we index Y_0 to Y_d the element in $\mathbb{F}_2^n$ of weight $\leq k-1$, where $d = \sum_{i=0}^{k-1}\binom{n}{i} - 1$.

Construction 3[6]: Let $n = 2k$ and $f \in \mathbb{B}_n$. The support of f is chosen in the following way:

- For $i = 0$ to $d-1$, choose $X_i \in [Y_i, Y_{i+1})$, and $wt(X_i) \leq n/2$;
- For $i = d$, choose $Y_i \preceq X_i$, and $wt(X_i) \leq n/2$;
- For $i = d+1$ to $2^{n-1}-1$, choose $X_i \notin \bigcup_{j=0}^{i-1}\{X_j\}$, and $wt(X_i) \leq n/2$.

Theorem 3: The functions $f(x)$ in construction 3 have optimal EAI.

Proof: Since $supp(f+1) \subseteq supp(f^c+1)$, $AN(f+1) \supseteq AN(f^c+1)$, because $f+1$ has the maximum AI, f^c+1 doesn't have annihilator of degree $< n/2$. One only needs to consider f^c. $f(x)$ is divided into two classes:

- $supp(f) \supseteq \{x | wt(x) < k\}$;
- $supp(f) \not\supseteq \{x | wt(x) < k\}$.

In the first class, because $f(x)$ is balanced, there must be x with weight k such that $f(x) = 1$. According to Theorem 1, f has maximum EAI.

In the second class, from the construction of f, if there exists a x with weight $< k$ such that $f(x) = 0$, then the weight of x must be $k-1$, and there must exists a corresponding vector y with property $wt(y) = k, x \preceq y, f(y) = 1$. Suppose $(i_1, i_2, \cdots, i_{k-1})$-th bits of x are 1 and others are 0, $(i_1, i_2, \cdots, i_k)$-th bits of y are 1 and others are 0. Let $\Omega = \{x | wt(x) = k\}$ and $\sharp\Omega = \frac{1}{2}\binom{n}{k}$, where $\sharp$ denotes the cardinality of a set, then $supp(f^c) = \{y\} \bigcup \{a | wt(a) < k \backslash \{x \bigcup 0\}\} \bigcup \Omega$. Let $g(x)$ is an annihilator of f^c, then $g(x) = 0$ for all $x \in supp(f^c)$. If $g(0) = 0$, from the proof of theorem 1, $g(x) = x_{i_1} x_{i_2} \cdots x_{i_{k-1}}$, but $g(y) = 1$, this is a contradiction, since $y \in supp(f^c)$. If $g(0) = 1$, from the proof of theorem 1, $g(x) = 1 + \sum_{i=1}^{n} x_i + \sum_{i<j} x_i x_j + ... + x_{k+2} \cdots x_n + x_{i_1} x_{i_2} \cdots x_{i_{k-1}}$, but $f(y) = 1$ and $g(y) = 0$. Denote $\Phi = \{z | x \preceq z, wt(z) = k\} \backslash \{y\}$, $\sharp\Phi = k$. It is easy to see $g(z) = 0, \forall z \in \Phi$. Since $\frac{1}{2}\binom{n}{k} > k$, there are must exists a vector α such that $f^c(\alpha) = 1$, and $x \not\preceq \alpha$, for this $\alpha, g(\alpha) = 1$. Then a contradiction is obtained. When there are two or more vectors such that

$f(x) = 1, x \in \{x|wt(x) = k-1\}$, it can prove it in the same way. So f^c doesn't have annihilator of degree $< k$. □

At the end of this paper, the extended algebraic immunity of functions constructed in [13] is studied:

Construction 4[13]: Let $n = 2k$ and $f \in \mathbb{B}_n, E = \{x|wt(x) > k\} \bigcup E', E' = \{x|wt(x) = k\}, |E'| = \frac{1}{2}\binom{n}{k}$,choose b such that $wt(b) = k-1, c \in E, b \preceq c, wt(c) + k = 1 mod 2$.then

$$f(x) = \begin{cases} 1, x \in \{b\} \bigcup E \backslash \{c\}; \\ 0, else. \end{cases}$$

It is evident that f^c doesn't have annihilator of degree $< k$. Similar to the proof of Theorem 1, when $wt(c) = k + i, i = 1 mod 2$, $f^c + 1$ doesn't have annihilator of degree $< k$ iff $\sum_{j=1}^{i}\binom{k+i}{j} = 1 mod 2 (1 \le i \le 2\lceil k/2 \rceil - 1, i = 1 mod 2)$. It is known that when k is even, $\sum_{j=1}^{i}\binom{k+i}{j} = 1 mod 2 (\forall i \in \{i|1 \le i \le 2\lceil k/2 \rceil - 1, i = 1 mod 2\})$, the functions have optimal EAI. When n is odd, if $i = k$, the condition is satisfied, f has maximum EAI. If $i \neq k$, by computer investigation we discover that when $k \le 25$, there are many cases such that $EAI(f) = k-1$, i.e., they don't have optimal extended algebraic immunity. Furthermore, we found that when $k = 5, 9, 17$, the functions don't have optimal EAI for all $i \in \{i|1 \le i \le 2\lceil k/2 \rceil - 1, i = 1 mod 2\}$ except $i = k$. So we conjecture that $i = k, i.e., wt(c) = n$ is the only function with optimal EAI in construction 4 when $k = 2^l + 1, l \ge 0$.

5 Conclusion

Because a difference of only 1 between the algebraic immunities of two functions can make a crucial difference with respect to algebraic attacks. Moreover, in an algebraic attack, one of course can compute $AI(f), AI(f^c), AI(f^r), AI(f^{rc})$, and obviously, they can apply the annihilators whose degree is lowest. So it is essential to analyze the extended algebraic immunity of known functions with optimal algebraic immunity.

Two sufficient conditions for a Boolean function with optimal EAI are given in this paper, then use them to study extended algebraic immunity of some known Boolean functions with optimal algebraic immunity. Using basic theory of linear algebraic, we study some other functions for their EAI. The results show that about half of them don't have optimal EAI. These results are helpful in analysis and construction of cryptographically significant Boolean functions. One should consider not only $AI(f)$, but also $EAI(f)$ and $EAI(f^r)$ when constructing cryptographically significant Boolean functions.

References

[1] A. Braeken and B. Preneel, On the algebraic immunity of symmetric Boolean functions, in Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2005, vol. 3797, pp. 35-48 [Online]. Available: http:// eprint.iacr.org/.

[2] C. Carlet and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2008, vol. 5350, pp. 425-440.

[3] N. Courtois, W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2003, vol. 2656, pp. 345-359.

[4] D. Dalai, S. Maitra, S. Sarkar, "Basic theory in construction of boolean functions with maximum possible annihilator immunity," Des. Codes Cryptogr., vol. 40, pp. 41-58 (2006).

[5] D. Dalai , S. Maitra, "Algebraic Immunity of Boolean Functions-Analysis and Construction," Computacin y Sistemas Vol. 12 No. 3, 2009, pp. 297-321.

[6] D. Dong, S. J. Fu, "A New Construction of Boolean Functions with Maximum Algebraic Immunity," in Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2009, vol. 5735, pp. 177-185.

[7] L. J. Qu, C. Li, and K. Feng, "A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2908-2910, Aug. 2007.

[8] L. J. Qu, K. Feng, F. Liu, and L. Wang, "Constructing Symmetric Boolean Functions With Maximum Algebraic Immunity," IEEE Trans. Inf. Theory, vol. 55, no. 5, pp. 2406-2412, May. 2009.

[9] P. Rizomiliotis, "On the Resistance of Boolean Functions Against Algebraic Attack Using Univariate Polynomial Representation," IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 4014-4024, Aug. 2010.

[10] Z. Tu and Y. Deng, "A Conjecture on Binary String and Its Applications on Constructing Boolean Functions of Optimal Algebraic Immunity," will appear in Des. Codes Cryptogr. May. 2010.

[11] C. Wang, X. Chen, "On extended algebraic immunity," Des. Codes Cryptogr. Accepted: 20 January. 2010.

[12] Q. Wang, J. Peng, H. Kan and X. Xue. "Constructions of cryptographiclly significant Boolean functions using primitive polynomials," in IEEE Trans. Inf. Theory, vol. 56, no. 6, pp. 3048-3053, June. 2010.

[13] W. Zhang, C. Wu and X. Liu, "Construction and enumeration of Boolean functions with maximum algebraic immunity," Sci China Ser F-Inf Sci. vol. 52 no. 1 pp. 32-40, Jan. 2009.

[14] X. M. Zhang, J. Pieprzyk, Y. Zheng, "On algebraic immunity and annihilators," in Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2006, vol. 4296, pp. 65-80.