Available online at www.sciencedirect.com

SciVerse ScienceDirect

IERI Procedia 2 (2012) 383 – 388

Procedia IERI

www.elsevier.com/locate/procedia

2012 International Conference on Future Computer Supported Education

Analysis of Extended Algebraic Immunity of Boolean Functions

Xiaowen Xiong*, Aiguo Wei , Zhuping Yang

Automobile Transportation Command Department, Military Transportation University, Tianjin, China

Abstract

Algebraic immunity (AI) is a new cryptographic criterion proposed against algebraic attacks. Extended algebraic immunity (EAI) extends the concept of algebraic immunity， whose point is that a Boolean function f may be replaced by another Boolean function f^c called the algebraic complement of f. In this paper, we investigate EAI of Boolean functions. Firstly, we present a sufficient and necessary condition to judge AI of a Boolean function equals to its EAI. Secondly, we prove that two classes of Boolean functions with maximum AI also have optimal EAI. Finally, we analyze that the structure of the annihilators of Boolean functions with the algebraic complement.

Keywords: Boolean functions; Algebraic attacks; Algebraic immunity; annihilators

1. Introduction

To resist algebraic attack[1], algebraic immunity(AI), has been introduced[2]. Then several constructions of Boolean functions with maximum AI (MAI) have been investigated[3-5]. In [3], Zhang etc. note that m sequence used frequently in stream ciphers doesn't have all zero states. Denoted an algebraic complement of f by f^c, then f and f^c have the same value for any $x \in F_2^n$ expect $x = 0$. Thus, if $AI(f^c) < AI(f)$, it is more efficient to take algebraic attacks after replacing f by f^c. Since a difference of only 1 between the algebraic immunities of two functions can make a crucial difference with respect to algebraic attacks, the

* Corresponding author. Tel.: +86-186-2208-6412
E-mail address: winnie101206@126.com.

 doi:10.1016/j.ieri.2012.06.105

difference between $AI(f)$ and $EAI(f)$ can not be ignored in algebraic attacks. So they extend the concept of AI, and define the extended algebraic immunity (EAI) of f as $EAI(f)=\min\{AI(f),AI(f^c)\}$. They prove that $0\le AI(f)-EAI(f)\le 1$ and show that $AI(f)-EAI(f)=1$ holds for a large number of cases. In [6], Wang etc. study the relation between different properties of f and f^c, such as weight, nonlinearity and so on. They also present a sufficient condition to judge $AI(f)=EAI(f)$. However, there are still many problems worth discussing. For example, it doesn't exist a sufficient and necessary condition to judge whether a Boolean function f satisfies $AI(f)=EAI(f)$. And we don't know whether a Boolean function f with MAI can also have optimal EAI.

In this paper, we study the above problems. The organization of the paper is as follows. In the following section we provide some necessary preliminaries of the paper. In Section Ⅲ, we present a sufficient and necessary condition to judge $AI(f)=EAI(f)$ firstly. Secondly, we prove that two classes of Boolean functions with MAI also have optimal EAI. Finally, we analyze the structure of the annihilators of Boolean functions with the algebraic complement. Section Ⅳ concludes the paper.

2. Preliminaries

Let F_2 be the binary finite field and F_2^n be the n-dimensional vector space over F_2. A Boolean function on n variables can be viewed as a mapping from F_2^n into F_2. Denote the set of all Boolean function on n variables by B_n. Any $f\in B_n$ can also be uniquely represented as a multivariate polynomial over F_2, called the algebraic normal form (ANF)

$$f(x_1,\ldots,x_n)=a_0+\sum_{i=1}^{n}a_ix_i+\sum_{1\le i<j\le n}a_{i,j}x_ix_ja_ix_i+\cdots+\sum_{1\le i_1<\cdots<i_d\le n}a_{i_1,\cdots,i_d}x_{i_1}\cdots x_{i_d}+\cdots+a_{1,\ldots,n}x_1x_2\cdots x_n.$$

where the coefficients are in F_2. The algebraic degree is the number of variables in the highest order term with nonzero coefficient and is denoted by $\deg(f)$. The support of $f\in B_n$ is denoted by $\mathrm{supp}(f)=\{x\in F_2^n \mid f(x)=1\}$. The Hamming weight of f, denoted by $wt(f)$, is defined as the number of ones in its truth table which equals to the size of $\mathrm{supp}(f)$. The function $f\in B_n$ is balanced if and only if $wt(f)=2^{n-1}$. Let $f,g\in B_n$, g is called an annihilator of f if $f\cdot g=0$. We denote the set of all annihilators of f by $AN(f)$. The algebraic immunity of f, denoted by $AI(f)$, is the minimum degree of all nonzero annihilators of f. Namely, $AI(f)=\min\{\deg(g)\mid 0\ne g\in AN(f)\cup AN(1+f)\}$. It is known that $AI(f)=\min\{\deg(f),\lceil n/2\rceil\}$ [1].

Definition 1 Given $f\in B_n$, we define an algebraic complement of f, denoted by f^c, as the function that contains all monomials $x_1^{u_1}\cdots x_n^{u_n}$,where each $u_j\in\{0,1\}$, that are not in ANF of the function f.

Definition 2 Given $f\in B_n$, the extended algebraic immunity of f, denoted by $EAI(f)$, is the minimum degree of nonzero Boolean functions in $AN(f)\cup AN(1+f)\cup AN(f^c)\cup AN(1+f^c)$, i.e.

$$EAI(f)=\min\{\deg(g)\mid 0\ne g\in AN(f)\cup AN(1+f)\cup AN(f^c)\cup AN(1+f^c)\}=\min\{AI(f),AI(f^c)\}.$$

Due to Definition 2, it's obvious that $EAI(f)\le\lceil n/2\rceil$.

Definition 3 Let $f\in B_n$, if the constant monomial in the ANF of f is zero (one) , we say f to be 0-CM (1-CM).

Property 1[3] Let $\Delta(x)=(1+x_1)\cdots(1+x_n)$, then the function $\Delta(x)$ has the following properties:

(1) $\Delta(x)=1$ if and only if $x=0$; (2) $f(x)\cdot\Delta(x)=0$ for $\forall f(x)\in B_n$ with $f(0)=0$;

(3) $f(x)\cdot\Delta(x)=\Delta(x)$ for $\forall f(x)\in B_n$ with $f(0)=1$.

Property 2[3] Let $f\in B_n$, then

(1) $f^c(x)=f(x)+\Delta(x)$ for all $x\in F_2^n$; (2) $f^c(x)=f(x)$ for all nonzero $x\in F_2^n$.

Due to Property 2, it's clear that $f(x)$ and $f^c(x)$ have different value just for $x=0$.

Property 3[3] Let $f\in B_n$, then

(1) $\left|AI(f)-AI(f^c)\right|\le 1$; (2) $0\le AI(f)-EAI(f)\le 1$, and $0\le AI(f^c)-EAI(f)\le 1$.

3. Main Results

3.1. A sufficient and necessary condition to judge $AI(f) = EAI(f)$

In [6], Wang etc. study the relation between $AI(f)$ and $EAI(f)$, but they can merely give a sufficient condition of $AI(f) = EAI(f)$. In the following part, we present a sufficient and necessary condition to judge $AI(f) = EAI(f)$ for the first time.

Lemma 1[6] Let $f \in \mathrm{B}_n$, then

(1) $AN(f^c) = AN(f) \cup AN(f)^c$ when f is 1-CM; (2) $AN(f) = AN(f^c) \cup AN(f^c)^c$ when f is 0-CM.

Corollary 1[6] Let $f \in \mathrm{B}_n$, then

(1) $AN(1+f) = AN(1+f^c) \cup AN(1+f^c)^c$ when f is 1-CM;

(2) $AN(1+f^c) = AN(1+f) \cup AN(1+f)^c$ when f is 0-CM.

Theorem 1 Let $f \in \mathrm{B}_n$, then

(1) When f is 0-CM, $EAI(f) = AI(f)$ if and only if $\forall 0 \neq g \in AN(1+f)$, $\deg(g^c) \geq AI(f)$.

(2) When f is 1-CM, $EAI(f) = AI(f)$ if and only if $\forall 0 \neq g \in AN(f)$, $\deg(g^c) \geq AI(f)$.

Proof. Firstly, we prove the sufficient condition. If for any $0 \neq g \in AN(1+f)$, $\deg g^c \geq AI(f)$. That is, for any $g \in AN(1+f)^c$, $\deg(g) \geq AI(f)$. Due to Corollary 1, we know that for any $g \in AN(1+f^c)$, $\deg(g) \geq AI(f)$. It is easy to see that f^c is 1-CM and $1+f$ is 1-CM when f is 0-CM, then $1+f^c$ is 0-CM. Note that for any $x \in F_2^n$, $f^c(x) = f(x) + \Delta(x)$. Then $(f + \Delta(x))g = fg + \Delta(x)g = 0$, if $f^c g = 0$. Note that f^c is 1-CM, that is $f^c(0) = 1$ when $x = 0$. So $g(0) = 0$. This implies that $\Delta(x)g \equiv 0$. Thus $fg = 0$. Hence for any $g \in AN(f^c)$, $\deg(g) \geq AI(f)$. Consequently, for any $g \in AN(1+f^c) \bigcup AN(f^c)$, $\deg(g) \geq AI(f)$. This implies that $AI(f^c) \geq AI(f)$. So $EAI(f) = AI(f)$.

Secondly, we prove the necessary condition. If $EAI(f) = AI(f)$, then $AI(f) \leq AI(f^c)$. So for any $0 \neq g \in AN(1+f^c) \cup AN(f^c)$, $\deg(g) \geq AI(f)$. That is, for any $g \in AN(f) \bigcup AN(1+f)$, $\deg(g^c) \geq AI(f)$. Therefore, for any $g \in AN(1+f)$, $\deg g^c \geq AI(f)$.

Thus, we finish the proof. □

The following result can be obtained directly from Theorem 1.

Corollary 2 Let $f \in \mathrm{B}_n$, then

(1) When f is 0-CM, $EAI(f) = AI(f) - 1$ if and only if $\forall 0 \neq g \in AN(1+f)$, $\deg(g^c) < AI(f)$.

(2) When f is 1-CM, $EAI(f) = AI(f) - 1$ if and only if $\forall 0 \neq g \in AN(f)$, $\deg(g^c) < AI(f)$.

3.2. The EAI of two classes of Boolean functions with MAI

To resist algebraic attacks more effectively, we hope the AI and EAI of Boolean functions can simultaneously achieve maximum. But in [6], it shows that a Boolean function on odd number of variables with MAI, can only satisfies $EAI(f) = \lfloor n/2 \rfloor$. In this subsection, we study the case of the Boolean functions on even number of variables. We research two classes of Boolean functions which satisfy $AI(f) = n/2$, and we give some sufficient and necessary conditions for them to achieve the maximum EAI at the same time.

Lemma 2[6] Let $f \in \mathrm{B}_n$, n even, and

$$f(x_1, \cdots, x_n) = \begin{cases} 0, wt(x_1, \cdots, x_n) < \frac{n}{2} \\ 1, wt(x_1, \cdots, x_n) > \frac{n}{2} \\ b \in \{0,1\}, wt(x_1, \cdots, x_n) = \frac{n}{2} \end{cases}.$$

Then $EAI(f) = n/2 - 1$ when $b = 1$.

Theorem 2 Let n even, a Boolean function

$$f(x_1,\cdots,x_n)=\begin{cases}0, wt(x_1,\cdots,x_n)<\frac{n}{2}\\ 1, wt(x_1,\cdots,x_n)>\frac{n}{2}\\ b\in\{0,1\}, wt(x_1,\cdots,x_n)=\frac{n}{2}\end{cases}.$$

Then $EAI(f)=n/2$, if and only if $\exists(x_1,\cdots,x_n)\in F_2^n$, s.t. $wt(x_1,\cdots,x_n)=n/2$ and $f(x_1,\cdots,x_n)=0$.

Proof. In [4], it has been proved that $AI(f)=n/2$. By Lemma 2, it is obvious to prove the necessary condition. Next we prove the sufficient condition.

Note that f is 0-CM, so it is just need to prove that $\forall g\in AN(1+f^c)$, $\deg(g)\geq n/2$. Let

$$f_1=1+f^c(x_1,\cdots,x_n)=\begin{cases}0, wt(x_1,\cdots,x_n)=0\\ 1, 1\leq wt(x_1,\cdots,x_n)<\frac{n}{2}\\ 0, wt(x_1,\cdots,x_n)>\frac{n}{2}\\ b+1\in\{0,1\}, wt(x_1,\cdots,x_n)=\frac{n}{2}\end{cases}.$$

Suppose that there exists $g\in B_n$, so as to $f_1g=0$ and $\deg(g)<n/2$. Then $g(x)=0$, when $1\leq wt(x_1,\cdots,x_n)<n/2$. Let $d=n/2-1$, then

$$g(x_1,\cdots,x_n)=g_0+\sum_{1\leq i\leq n}g_ix_i+\sum_{1\leq i<j\leq n}g_{ij}x_ix_j+\cdots+\sum_{1\leq i_1<i_2<\cdots<i_d\leq n}g_{i_1i_2\cdots i_d}x_{i_1}x_{i_2}\cdots x_{i_d}.$$

When $wt(x_1,\cdots,x_n)=1$, $g(x)=0=g_0+g_i$. Then for any $1\leq i\leq n$, $g_i=g_0$.
When $wt(x_1,\cdots,x_n)=2$, $g(x)=0=g_0+g_i+g_j+g_{ij}$.
Then for any $1\leq i<j\leq n$, $g_{ij}=g_0$. In the same way, when $wt(x_1,\cdots,x_n)=d$, $g(x)=0=\sum_{\mathrm{supp}(I)\subseteq\mathrm{supp}(x)}g_I$.

Then for any $1\leq i_1<i_2<\cdots<i_d\leq n$, $g_{i_1i_2\cdots i_d}=g_0$. Thus

$$g(x_1,\cdots,x_n)=g_0(1+\sum_{1\leq i\leq n}x_i+\sum_{1\leq i<j\leq n}x_ix_j+\cdots+\sum_{1\leq i_1<i_2<\cdots<i_d\leq n}x_{i_1}x_{i_2}\cdots x_{i_d}).$$

If $g_0=1\neq 0$, then $g(x_1,\cdots,x_n)=1+\sum_{1\leq i\leq n}x_i+\sum_{1\leq i<j\leq n}x_ix_j+\cdots+\sum_{1\leq i_1<i_2<\cdots<i_d\leq n}x_{i_1}x_{i_2}\cdots x_{i_d}$.
When $wt(x_1,\cdots,x_n)=n/2$,

$$g(x)=\sum_{\mathrm{supp}(I)\subseteq\mathrm{supp}(x)}g_I=(2^{n/2}-1)=1\neq 0.$$

It has been already known that there exists $(x_1,\cdots,x_n)$, so as to $wt(x_1,\cdots,x_n)=n/2$ and $f(x_1,\cdots,x_n)=0$, thus $f_1(x_1,\cdots,x_n)=1$. But this contradicts the fact that $f_1g=0$. So $g_0=0$ and $g(x)=0$. Hence, when $AI(f)=n/2$, it must be $g=0$ or $\deg(g)\geq n/2$ if $(1+f^c)g=0$. That is, $\deg g^c\geq AI(f)$ for any $g\in AN(1+f)$. Then by Theorem 1, $EAI(f)=n/2$, this finishes the proof. □

Theorem 3 Let n be any even such that $n\geq 2$ and α a primitive element of the field F_2^n. Let f be the Boolean function on F_2^n whose support is $\{0\}\bigcup\{\alpha^i\,|\,i=0,1,\cdots,2^{n-1}-2\}$. Then $EAI(f)=n/2$.

Proof. In [5], it has been proved that $AI(f)=n/2$. Note f is 1-CM, so it is just need to prove that $\forall g\in AN(f^c)$, $\deg(g)\geq n/2$.

Let g be any Boolean function of algebraic degree at most $n/2-1$. Let $g(x)=\sum_{i=0}^{2^n-1} g_i x^i$ be its univariate representation in the field F_2^n, where $g_i \in F_2^n$ is null if the 2-weight $w_2(i)$ of i is at least $n/2$ (which implies in particular that $g_{2^{n-1}}=0$).

If g is an annihilator of f^c, then we have $g(\alpha^i)=0$ for every $i=0,1,\cdots,2^{n-1}-2$, that is, the vector $(g_0,\cdots,g_{2^n-2})$ belongs to the Reed-Solomon code over F_2^n of zeroes $1,\alpha,\cdots,\alpha^{2^{n-1}-2}$. If g is non-zero, then by definition, we have

$$\begin{pmatrix} g(1) \\ g(\alpha) \\ \vdots \\ g(\alpha^{2^n-2}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{2^n-2} & \alpha^{2(2^n-2)} & \cdots & \alpha^{(2^n-2)(2^n-2)} \end{pmatrix} \times \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{2^n-2} \end{pmatrix}.$$

which implies (since for every $0 \le i, j \le 2^n-2$, the sum $\sum_{k=0}^{2^n-2} \alpha^{(i-j)k}$ equals 1 if $i=j$ and 0 otherwise):

$$\begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{2^n-2} \end{pmatrix} == \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{-(2^{n-1}-1)} & \alpha^{-2^{n-1}} & \cdots & \alpha^{-(2^n-2)} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha^{-(2^{n-1}-1)(2^n-2)} & \alpha^{-2^{n-1}(2^n-2)} & \cdots & \alpha^{-(2^n-2)(2^n-2)} \end{pmatrix} \times \begin{pmatrix} g(\alpha^{2^{n-1}-1}) \\ g(\alpha^{2^{n-1}}) \\ \vdots \\ g(\alpha^{2^n-2}) \end{pmatrix}$$

Suppose that at least 2^{n-1} of the g_i 's are null. Then, $g(\alpha^{2^{n-1}-1}), g(\alpha^{2^{n-1}}), \cdots, g(\alpha^{2^n-2})$ satisfy a homogeneous system of linear equations whose matrix is a $2^{n-1} \times 2^{n-1}$ Vandermonde matrix and whose determinant is therefore non-null. This implies that $g(\alpha^{2^{n-1}-1}), g(\alpha^{2^{n-1}}), \cdots, g(\alpha^{2^n-2})$ are null. And therefore g must then be null, a contradiction. Hence the vector $(g_0,\cdots,g_{2^n-2})$ has weight at least 2^{n-1}. Moreover, suppose that this vector has Hamming weight 2^{n-1} exactly. Since the number of integers of 2-weight at most $\lceil n/2 \rceil - 1$ is not strictly greater than 2^{n-1}, then $g(x)=\sum_{0 \le i \le 2^n-2, w_2(i) \le (n-1)/2} x^i$ and n is odd, but this contradicts the fact that $g(0)=0$. We deduce that the vector $(g_0,\cdots,g_{2^n-2})$ has Hamming weight strictly greater than 2^{n-1}, leading to a contradiction with the fact that g has algebraic degree at most $deg(g) \le n/2-1$. Hence $g(x)=0$, that is, there does not exist a non-zero annihilator of f^c of algebraic degree at most $n/2-1$. Thus $EAI(f)=n/2$. □

3.3. A new method to analyze the structure of $AN(f)$

The annihilators of Boolean functions play a very important part in algebraic attacks. If the Boolean functions f and $1+f$ have annihilators with lower algebraic degree, it will effectively improve efficiency of algebraic attacks. Consequently, we wish that we can find an effective algorithm to obtain annihilators of a Boolean function and judge a Boolean function whether exists annihilators with lower algebraic degree. In search of annihilators with lower algebraic degree, it's very useful to analyze the structure of the annihilators of Boolean functions. Next, by using relation between annihilator sets of f and f^c, we present a new method to characterize the structure of the annihilators of Boolean functions.

Let $S \subseteq F_2^n$, and define

$$f^s(x)=\begin{cases} f(x), x \notin S \\ f(x)+1, x \in S \end{cases}.$$

Denote $\Delta_s(x)=\sum_{a=(a_1,\cdots,a_n)\in S}\prod_{i=1}^{n}(x_i+a_i+1)$, then $f^s(x)=f(x)+\Delta_s(x)$.

Theorem 4 Let r be any positive integer, and $I=\{x\in F_2^n \,|\, wt(x)\le r, f(x)=0\}$ .Then

$$AN(f)=\bigcup_{S\subseteq I}(AN(f^I))^S .$$

Proof. One hand, if $g\in AN(f)$, then $fg=0$. Thus $g=0$ when $x\in \mathrm{supp}(f)$. Let $S_0=\{x\in I \,|\, g(x)=1\}\subseteq I$ and $\varphi(x)=g(x)^{S_0}$, then

$$\varphi(x)=\begin{cases}0, x\in I\\ g(x), x\notin I\end{cases}.$$

So $\varphi(x)f^I(x)=0$, that is $\varphi(x)\in AN(f^I)$. Then $g(x)\in\bigcup_{S\subseteq I}(AN(f^I))^S$. Hence $AN(f)\subseteq\bigcup_{S\subseteq I}(AN(f^I))^S$. On the other hand, if $g\in\bigcup_{S\subseteq I}(AN(f^I))^S$, there exists $S_0\subseteq I$, so as to $g\in(AN(f^I))^{S_0}$. Then $g^{S_0}\in AN(f^I)$, that is, $g^{S_0}f^I=0$. Note that $(g^{S_0})^{S_0}=g$, $S_0\subseteq I$ and for any $x\in I$, $f(x)=0$. Then $gf=0$. So $g\in AN(f)$. Hence $\bigcup_{S\subseteq I}(AN(f^I))^S\subseteq AN(f)$.

Therefore $AN(f)=\bigcup_{S\subseteq I}(AN(f^I))^S$, it completes the proof. □

Theorem 4 presents a new method to characterize the structure of $AN(f)$. This method conduces to obtain all the elements of $AN(f)$. According to the definition of the set I in theorem 4, if $x\in F_2^n$ and $wt(x)\le r$, then $f^I(x)=1$. Hence, $AN(f^I)$ is more easily to gain than $AN(f)$. After finding all the elements of $AN(f^I)$, for any $S\subseteq I$ and $g\in AN(f^I)$, we compute $g^s(x)=g(x)+\Delta_s(x)$, then we will obtain all the elements of $AN(f)$. Note that the number of subset of I increases with index growth of $|I|$, so r can not choose too large. This method is quite possible to offer a faster way to compute AI, once there is an effective way to obtain lower elements in $AN(f^I)^S$. That is our future study.

4. Conclusion

In this paper, we study some results on EAI of Boolean functions. By the relation between annihilator sets of f and f^c, we present a sufficient and necessary condition to judge $AI(f)=EAI(f)$ for the first time. Next, we prove that two classes of Boolean functions with MAI also have optimal EAI. Finally, we analyze the structure of the annihilators of Boolean functions with the algebraic complement. Furthermore, there are still some problems need to be studied. For example, how to improve the efficiency of the sufficient and necessary condition presented in this paper, and how to construct Boolean functions with maximum EAI to resist fast algebraic attacks.

References

[1] N. Courtois, W. Meier. “Algebraic attacks on stream ciphers with linear feedback”, Cryptology-EUROCRYPT 2003, 2003, LNCS 2656: 345-359.

[2] W. Meier, E. Pasalic, C. Carlet. “Algebraic attacks and decomposition of Boolean functions”, Cryptology-EUROCRYPT 2004, 2004, LNCS 3027: 474-491.

[3] X.M. Zhang, P. Josef, Y.L. Zheng. “On algebraic immunity and annihilators”, ICISC 2006, 2006, LNCS 4296: 65-80.

[4] D.K. Dalai. “Basic theory in construction of Boolean functions with maximum possible annihilator immunity”, Designs, Codes and Cryptography, 2006, 40(1): 41-58.

[5] C. Carlet and K.Q. Feng. “An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity”, ASIACRYPT 2008, 2007, LNCS 5350: 425-440.

[6] C.P. Wang, X.S. Chen. “On extended algebraic immunity”, Designs, Codes and Cryptography, 2010, 57(3): 271-281.