TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.4, April 2014, pp. 3010 ~ 3014
DOI: http://dx.doi.org/10.11591/telkomnika.v12i4.4773

On the Algebraic Immunity of Boolean Function

Cao Hao*, Wang Huige
College of Science, Anhui Science and Technology University, Feng yang 233100, China
*Corresponding author, email: caohao2000854@163.com

Abstract

In view of the construction requirements of Boolean functions with many good cryptography properties, through the analysis of the relationship between the function values on the vectors with weight not more than d and the algebraic immunity, a method to determine the higher order algebraic immunity function is given. Meanwhile, a method that appropriate change in the function value without reducing algebraic immunity is produced, and using it, an example to construct Boolean function with optimal properties in the algebraic immunity, nonlinearity, balance and correlation immunity etc is presented.

***Keywords**: Boolean function, algebraic immunity (AI), support set, corelation immunity (CI), nonlinearity*

1. Introduction

As an important tool in the designing and analysis of cryptosystem, Boolean function has been a research focus in cryptography. To resist variable known attacks, a variety of cryptographic properties have been put forward, such as correlation immunity, balancedness, nonlinearity, etc. In 2003, a new clever attack on stream ciphers, the so called algebraic attack [1], which is based on the solving overdetermined nonlinear multivariable equations between the initial key and the outputs of Key Stream Generator (KSG), brings a completely new criterion for the design of secure stream cipher systems, known as algebraic immunity (AI) [2, 3]. To resist algebraic attack, algebraic immunity of Boolean function cannot be too low. Hence, it is very meaningful to construct Boolean functions with high AI. Being based on the study of algebraic attacks, scholars have already presented many constructions of Boolean functions with high AI by using different approaches [3-15]. However, it is still a difficult problem to meeting various other good cryptographic properties when constructing Boolean functions with high AI.

In this paper, having deeply studied on the relations between the AI and the Support set of Boolean functions, a sufficient condition that modifying several values of the Boolean function in some point does not decrease AI is presented. Using this method, construction of Boolean functions with good cryptographic properties, such that algebraic immunity, balancedness, nonlinearity and correlation immunity, is presented.

2. Preliminary

A function $f:\{0,1\}^n \rightarrow \{0,1\}$ is called n-variable Boolean function. We denote B_n the set of all n-variable Boolean functions from $\{0,1\}^n$ to $\{0,1\}$. Denote 0_f = {x {0,1}n | f (x)= 0} and 1_f = {x {0,1}n | f (x)= 1}, which are called off set and support set.

Any n-variable Boolean function has a unique representation as a multivariate polynomial over *GF*(2), called algebraic normal form (ANF) :

$$f(x_1,x_2,\ldots,x_n)=a_0 \underset{1\le i\le n}{\oplus} a_i x_i \underset{1\le i<j\le n}{\oplus} a_{i,j}x_i x_j \oplus\cdots\oplus a_{1,2,\cdots,n}x_1x_2\cdots x_n \qquad (1)$$

Where the coefficients $a_{i_1 i_2\cdots i_k}\in GF(2)$ and ⊕ denote the *GF*(2) addition. The algebraic degree, deg(*f*), is the number of variables in the highest order term with nonzero coefficient. In the ANF of f(x), it is satisfied that:

Received September 10, 2013; Revised November 18, 2013; Accepted December 1, 2013

$$a_{i1,i2,\cdots,ij} = \underset{\sup(x)\subseteq\{i1,i2,\cdots,ij\}}{\oplus} f(x) \qquad (2)$$

Where sup(x) denotes the serial numbers of 1 in $x=(x_1,x_2,\ldots,x_n)$, i.e., $\sup(x)=\{i|x_i=1\}$.

An important tool to study the cryptographic properties of Boolean functions, called Spectrum (denoted by $S_f(w)$), is defined as:

$$S_f(w) = 2^{-n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+wx}, \quad (w\in\{0,1\}^n) \qquad (3)$$

Nonlinearity of Boolean function is an important Cryptograph index, which is defined as the minimum distance between the function and all affine functions, denoted by N_f. It can be depicted by the equation as follows:

$$N_f = 2^{n-1}(1-\max\{|S_f(w)|, w\in\{0,1\}^n\} \qquad (4)$$

An n-variable Boolean function f is called m-order correlation immune, if for any $w\in F_2$ with $1\leq wt(w)\leq m$, we have $S_f(w)=0$, where $wt(w)$ denotes the Hamming weight of w. Further more, if $S_f(0)=0$(i.e., f is balanced), f is called m-order resilient Boolean function. The relation between the number of variables, algebraic degree and correlation immunity can be described as follows:

$$m+n\leq d \qquad (5)$$

If f is balanced, we have $m+n<d$.

Let $f(x)$, $g(x)\in B_n$, $g(x)$ is called an annihilator of f if $f(x)\cdot g(x)=0$ for all $x\in\{0,1\}^n$, denoting An(f) as the set of all annihilators of f. The algebraic immunity of f is defined as follows:
$AI(f)=\min\{g\in B_n \mid g\in Ann(f)\cup Ann(1+f) \text{ and } g\neq 0\}$

It is known that for arbitrary n-variable Boolean function f, we have $AI(f)\leq n/2$[3]. To resist algebraic attack, combination function with high AI should be selected in the design of KSG. Therefore, constructing Boolean functions with optimal AI is necessary.

3. Judging the AI of Boolean Function

Denote $W_{<d}=\{x\ \ \{0,1\}n|wt(x)<d\}$, $W_{>d}=\{x\ \ \{0,1\}n|wt(x)>d\}$, $W_{=d}=\{x\ \ \{0,1\}n|wt(x)=d\}$. For any $f\in B_n$, denote $W_{<d}\cap 0_f = \{\alpha_1,\alpha_2,\ldots,\alpha_s\}$, $W_{=d}\cap 0_f= \{\gamma_1,\gamma_2,\ldots,\gamma_m\}$, $W_{>d}\cap 1_f = \{\beta_1,\beta_2,\ldots,\beta_t\}$, $W_{=d}\cap 1_f = \{\xi_1,\xi_2,\ldots,\xi_k\}$. Construct two matrix $A=(a_{ij})_{m\times s}$ and $B=(b_{ij})_{k\times t}$, where a_{ij} =1if and only if $\sup(\alpha_j)\subseteq\sup(\gamma_i)$, and b_{ij}=1 if and only if $\sup(\xi_j)\subseteq\sup(\beta_i)$. On the AI of Boolean function, we have the following conclusion:

Theorem 1: A and B are all column full rank matrix $\Rightarrow$ AI(f)≥d.

Proof: Firstly, we only show that f does not exist non-zero annihilator with degree no more than d-1.

For any $g(x)\in An(f)$ with $\deg(g)\leq d-1$, we show that g(x)=0. From Equation (2), it is known that if $\forall x\in W_{<d}$, then $g(x)=0$. It is obvious that when $x\in W_{<d}\cap 1_f$, we have:

$$g(x)=0 \qquad (6)$$

Now, we show that the equation g(x)=0 still holds if $x\in W_{<d}\cap 0_f$.
Owing to $\deg(g)\leq d-1$, we have $\underset{\sup(x)\subseteq\sup(\gamma_i)}{\oplus} g(x)=0$ for any $\gamma_i\in W_{=d}\cap 0_f$. From the Equation (6) and the definition of matrix A, we have $\oplus_{j=1}^{s} a_{ij}\, g(\alpha_j)=0$. Therefore, we can get equations containing m homogeneous linear equations on variables $g(\alpha_1),g(\alpha_2),\ldots,g(\alpha_s)$, and the coefficient matrix of the equations A is column full rank. Obviously, the equations only has a zero solution, i.e., $g(x)=0$ also holds when $x\in W_{<d}\cap 0_f$. Hence, f does not exist non-zero annihilator with degree no more than d-1.

Next, we show that 1⊕f does not exist non-zero annihilator with degree no more than d-1. For any g(x) ∈An(1⊕f) with deg(g)≤d-1. Denote g'(x)=g(1⊕x), it needs only prove that g'(x)=0, we will get g(x)=0. Similar to the previous proof method, we will get g'(x)=0, hence, g(x)=0, that is to say, 1⊕f does not exist non-zero annihilator with degree no more than d-1.

Therefore, Neither f nor 1⊕f exist non-zero annihilator with degree no more than d-1, namely AI(f)≥d.

4. Constructing Boolean Functions with high AI

Select $T\subseteq W_{<d}\cap 1_f$, $U\subseteq W_{=d}\cap 0_f$, $S\subseteq W_{>d}\cap 0_f$, $V\subseteq W_{=d}\cap 1_f$, denote $(W_{<d}\cap 0_f)\cup T = \{\alpha_{t1},\alpha_{t2},\ldots,\alpha_{tl1}\}$, $U=\{\gamma_{u1},\gamma_{u2},\ldots,\gamma_{ul2}\}$, $(W_{>d}\cap 1_f)\cup S= \{\beta_{s1},\beta_{s2},\ldots,\beta_{sl3}\}$, $V= \{\xi_{v1},\xi_{v2},\ldots,\xi_{vl4}\}$, where $l_1\le l_2$, $l_3\le l_4$. Define two matrix M and N as follows: $M=(m_{ij})_{l2\times l1}$ and $N=(n_{ij})_{l4\times l3}$, where m_{ij}=1if and only if $\sup(\alpha_{tj})\subseteq\sup(\gamma_{ui})$ and n_{ij}=1if and only if $\sup(\xi_{vj})\subseteq\sup(\beta_{si})$. We have the follow conclusion:

Theorem 2: Let $f\in B_n$ with AI(f)=d. Define $h(x)$:

$$h(x)=\begin{cases} 1 & x\in S\cup U \\ 0 & x\in T\cup V \\ f(x) & otherwise \end{cases}$$

If M and N are all column full rank matrix, Then AI(h)≥d.

Proof: Firstly, we show that h does not exist non-zero annihilator with degree no more than d-1.

For any g(x) ∈An(h) with deg(g)≤d-1, we show that g(x)=0. From Equation (2), it is known that if $\forall x\in W_{<d}$, then $g(x)$=0. It is obvious that when $x\in W_{<d}\cap 1_h$, we have:

$$g(x)=0 \qquad (7)$$

Now, we only show that the equation g(x)=0 still holds if $x\in W_{<d}\cap 0_h = (W_{<d}\cap 0_f)\cup T$. Owing to deg(g)≤d-1, we have $\bigoplus_{\sup(x)\subseteq\sup(\gamma_{ui})} g(x)=0$ for any $\gamma_{ui}\in U$. From the Equation (7) and the definition of matrix M, we have $\bigoplus_{j=1}^{l1} m_{ij}\, g(\alpha_{tj})=0$. Therefore, we can get equations containing l_2 homogeneous linear equations on variables $g(\alpha_{t1}),g(\alpha_{t2}),\ldots,g(\alpha_{tl1})$, and the coefficient matrix of the equations M is column full rank. Obviously, the equations only has a zero solution, i.e., $g(x)$=0 also holds when $x\in W_{<d}\cap 0_f$. Hence, h does not exist non-zero annihilator with degree no more than d-1.

Next, we show that 1⊕f does not exist non-zero annihilator with degree no more than d-1. For any g(x) ∈An(1⊕f) with deg(g)≤d-1. Denote g'(x)=g(1⊕x), it needs only prove that g'(x)=0, we will get g(x)=0. Similar to the previous proof method, we will get g'(x)=0, hence, g(x)=0, that is to say, 1⊕f does not exist non-zero annihilator with degree no more than d-1.

Therefore, Neither f nor 1⊕f exist non-zero annihilator with degree no more than d-1, namely AI(f)≥d.

Similar to the previous proof method, we will get that 1⊕h does not exist non-zero annihilator with degree no more than d-1.

Therefore, Neither h nor 1⊕h exist non-zero annihilator with degree no more than d-1, namely AI(h)≥d.

Using **Theorem 2**, we can construct a class of Boolean functions with AI no less than d from a given Boolean function *f* with AI(f)=d. For example, let *f*(*x*) be a n-variable Majority Boolean function, where n is even, we can construct Boolean functions with good cryptographic properties.

5. Example of Constructing Boolean Functions with Good Cryptographic Properties

In this section, we will present a example of constructing a 4-variable Boolean functions with good cryptographic properties.

Example: Let n=4 and d=2 in **Theorem 2**, and select a majority function f(x) randomly. The function values and spectrum of f(x) can be described by the following table:

Table 1. The Function Values and Spectrum of f(x)

w	0000	0001	0010	0011	0100	0101	0110	0111
f(w)	1	1	1	0	1	1	0	0
$S_f(w)$	0	-1/4	-1/2	1/4	-1/2	-1/4	0	1/4
w	1000	1001	1010	1011	1100	1101	1110	1111
f(w)	1	1	1	0	0	0	0	0
$S_f(w)$	-1/4	0	-1/4	0	1/4	0	1/4	0

From the table, it could easily get that N_f=4. The The N_f is high, and is close to Bent function(the Nonlinearity of 4-variable Bent function is 6). According to calculations, we get the ANF of f(x) as follows:

$$f(x)=x_1x_2x_4+x_1x_3x_4+x_1x_2+x_2x_3+x_3x_4+1$$

Select T={0000,0001}, U={0011,1100}, S={0111,1011,1101} and V={0101,1010,1001}, then we will get the matrix M and N which are induced by T, U, S and V as follows:

$$M=\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}, \qquad N=\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 1 & 1\end{bmatrix}$$

Because the matrix M and N are all column full rank matrix, so the AI of the Boolean function h(x) decided by **Theorem 2** is optimal.

Next, we discuss any other properties of h(x). According to calculations, we get the table which can present the function values and spectrum of h(x).

Table 2. The Function Values and Spectrum of h(x)

w	0000	0001	0010	0011	0100	0101	0110	0111
h(w)	0	0	1	1	1	0	0	1
$S_h(w)$	0	0	0	-1/2	0	0	1/2	0
w	1000	1001	1010	1011	1100	1101	1110	1111
h(w)	1	0	0	1	1	1	0	0
$S_h(w)$	0	0	1/2	0	0	0	0	1/2

It is easily to get that N_h=4. From the table, we can see the spectrum of h(x) on the vectors with weight not morn than 1 are all 0, so h(x) is a 1-resilient Boolean function. From Equation (5), It is easy to get that the resiliency of h(x) is optimal among all the nonlinear functions. Therefore h(x) achieves optimal in many cryptographic properties, such as balancedness, algebraic immunity, nonlinearity, and correlation immunity.

6. Conclusion

We proposed a sufficient condition that modifying several values of the Boolean function in some point does not decrease AI, and presented a construction of 4-variable Boolean function with good cryptographic properties, such that algebraic immunity, balancedness, nonlinearity and correlation immunity. However, how to effectively select the point (and then modify the values of these points) is a difficult problem. If this problem could be effectively solved, it will be meaningful to the construction of cryptosystem with high security, and it is also the further research.

Acknowledgements

The paper is supported by **NCFS** (60573026); Anhui Province Natural Science Research Project (KJ2010B059); Anhui Province Natural Science Research Project (KJ2013B083); Anhui Provincial Natural Science Foundation (1208085QF119).

References

[1] Courtois N, Meier W. Algebraic attacks on stream cipherswith linear feedback. *Advances in Cryptology-Eurocrypt*. Berlin. 2003; 2656: 345 - 359.
[2] Armkneckt F. Improving fast algebraic attacks. *Fast Software Encryption.* Delhi. 2004; 3017: 65 - 82.
[3] Courtois N. Fast algebraic attacks on stream ciphers with linear feedback, *Advances in Cryptology-Crypto*. California. 2003; 2729: 176-194.
[4] Dalai DK, Maitra S, Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. *Designs Codes and Cryptography*. 2006; 40(1): 41-58.
[5] Zepeng Z, Jinfeng C, Guozhen X, Hao C. Spectral Analysis of Two Boolean Functions and Their Derivatives. *Chinese Journal of Electronics*. 2011; 20(4): 747-749.
[6] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions. *Advances in Cryptology-Eurocrypt*. Berlin. 2004; 3027: 474-491.
[7] Weiguo Z, Yong D, Ning D, Guozhen X. A Characterization of Algebraic Immune Boolean Functions. *Journal of Beijing University of Posts and Telecommunications*. 2007; 30(5): 55-57.
[8] Qiang M, Lu Sheng C, Fang Wei F. Construction of Boolean Functions with Maximum Algebraic Immunity. *Journal of Software*. 2010; 21(7): 1758-1767.
[9] Xiaowen X, Ai-guo W, Zhi-jun Z. Construction of Rotation Symmetric Boolean Functions with Good Cryptographic Properties. *Journal of Electronics & Information Technology*. 2012; 34(10): 2358-2362.
[10] Yong-juan W, Shi-wu Z. Construction of Boolean functions with optimum algebraic immunity. *Journal of Computer Applications*. 2012; 32(1): 49-51, 73.
[11] Guangpu G, Wen-fen L. The Notes on the Linear Structures of Rotation Symmetric Boolean Functions. *Journal of Electronics & Information Technology*. 2012; 34(9): 2273-2276.
[12] Yongtao P, Wenfeng Q. Construction of Balanced Correlation-Immune Functions with Highest Degree. *Journal of Electronics & Information Technology*. 2006; 28(12): 2355-2358.
[13] Chuanda Q, Ying-da Y. Algebraic Degree of a Class Boolean Function Annihilators. *Acta Electronica Sinica.* 2012; 40(6): 1177-1179.
[14] Hao C, Shimin W, Huige W. Constructions of odd variables symmetric boolean functions with second-order correlation immunity. *Computer Engineering and Applications*. 2012; 48(2): 83-85.
[15] Jiao M, Qiaoyan W. Constructions of Boolean Functions with Optimal Algebraic Immunity. *Journal of Beijing University of Posts and Telecommunications.* 2009; 32(4): 73-76.