Asian Journal of Information Technology 9 (3): 179-182, 2010
ISSN: 1682-3915

Construction and Count of Balanced Algebraic Immune Boolean Functions with Lobanov's Bound of Nonlinearity

[1]Qian-Qiong Wu and [2]Ming Duan
[1]Department of Electrical Engineering and Automation,
Luoyang Institute of Science and Technology, Luoyang, China
[2]Department of Basic Courses, University of Foreign Language, Luoyang, China

Abstract: Recently Lobanov's tight bound of nonlinearity of balanced algebraic immune Boolean functions has received a lot of attention in cryptographic literature. In this study a general construction of balanced algebraic immune Boolean functions was given with the nonlinearity bound. Moreover from the construction, we get a lower bound of the count of balanced algebraic immune functions was got with the nonlinearity bound. As far as we know, this is the first bound about this count.

Key words: Algebraic attack, algebraic immunity, nonlinearity, Boolean function, balanced algebraic, immune, China

INTRODUCTION

Recently algebraic attack is received a lot of attention in cryptography (Courtois and Meier, 2002; Dalai *et al*., 2004a, b; Lobanov, 2005; Carlet *et al*., 2006). A new cryptographic criterion, algebraic immunity is given to resist this attack. Subsequently the combinations among algebraic immunity and other requirements to Boolean functions exploited as nonlinear filters in stream ciphers are studied. More respect was given in the problem of the relations between algebraic immunity and nonlinearity of Boolean functions.

Dalai *et al*. (2004a, b) was proved the lower bound for the nonlinearity of a Boolean function via its algebraic immunity. The result showed that a Boolean function with low nonlinearity will have low algebraic immunity. Lobanov (2005) has shown the stronger tight lower bound for the nonlinearity of a Boolean function via its algebraic immunity and construct balanced Boolean functions with this bound for all possible values of parameters.

In this study we give a more general construction of these balanced algebraic immunity Boolean functions that with Lobanov's bound for all possible values of parameters and take the previous construction as an example. Furthermore from the construction it can get a lower bound of the count of balanced algebraic immune functions with Lobanov's bound. As far as we know, this is the first bound about this count.

PRELIMINARIES

A Boolean function of n variable is a mapping f: $F_2^n \rightarrow F_2$ where F_2 is the field of two elements. Any Boolean function has its Algebraic Normal Form (ANF):

$$f(x_1,\cdots,x_n) = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1\le i\le j\le n} a_{ij} x_i x_j + \cdots + \sum_{1\le i_1\le\cdots\le i_k\le n} a_{i_1\cdots i_k} x_{i_1}\cdots x_{i_k}$$

where, $a_0,\ldots,a_{i_1\cdots i_k} \in F_2$. The algebraic degree of f is the number of variables in the highest order term in the above ANF. The weight wt (x) of a vector x in F_2^n is the number of ones in x.

Definition 1: If f_1 and f_2 are Boolean functions of n variable then the distance between f_1 and f_2 is defined as:

$$d(f_1,f_2) = \left|\left\{x \in F_2^n \,\middle|\, f_1(x) \neq f_2(x)\right\}\right|$$

Definition 2: If f is a Boolean function of n variable then the nonlinearity nl (f) of f over F_2^n is defined as:

$$nl(f) = \min_{l,\deg(l)\le 1} d(f,l)$$

Definition 3: If f is a Boolean function of n variable then for any vector $u \in F_2$, the Walsh coefficient of f at u is:

Corresponding Author: Qian-Qiong Wu, Department of Electrical Engineering and Automation,
Luoyang Institute of Science and Technology, Luoyang, China

$$W_f(u) = \sum_{x \in F_2^n} (-1)^{f(x)+\langle u,x \rangle}$$

The nonlinearity is expressed via Walsh coefficients by the next formula:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{u \in F_2^n} |W_f(u)|$$

Definition 4: For a given n-variable Boolean function f, a nonzero n-variable Boolean function g is called an annihilator of f if f.g = 0 and the algebraic immunity of f denoted by AI (f) is the minimum value of d such that f or f+1 admits an annihilating function of degree d. Dalai *et al.* (2004a) proved that if:

$$nl(f) < \sum_{i=0}^{d} \binom{n}{i}$$

then Al (f)≤d+1. This is equivalent to the lower bound of nonlinearity:

$$nl(f) \geq \sum_{i=0}^{AI(f)-2} \binom{n}{i}$$

Lobanov (2005) improved the result.

Lemma 1 (Lobanov's bound). Let $f(x_1,\ldots,x_n)$ be a Boolean function over F_2^n and AI(f) = k then:

$$nl(f) \geq 2^{n-1} - \sum_{i=k-1}^{n-k} \binom{n-1}{i} = 2\sum_{i=0}^{k-2} \binom{n-1}{i}$$

Definition 5: A boolean function f(x) is called self-dual if $f(x_1+1,\ldots, x_n+1) = f(x_1, \ldots, x_n)+1$.

It is easy to see that if f is self-dual then the fact that f has not a nonzero annihilator of degree less than k follows that f +1 has not a nonzero annihilator of degree less than k too. Therefore the minimum degrees of nonzero annihilators of functions f and f+1 are the same. Thus, for the finding of algebraic immunity of a self-dual function f it is sufficient to consider only annihilators of the function f.

CONSTRUCTION AND COUNT

Combination foundation: First, an important theorem in combination for the construction was shown.

Lemma 2: For any natural number n and i, 0≤i≤n

$$\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$$

Lemma 3: For any natural number n and k, 0≤k<n

$$\sum_{i=0}^{k-2} \binom{n-1}{i} = \sum_{j=0}^{1} \binom{1}{j} \sum_{i=0}^{k-2-j} \binom{n-2}{i}$$

Proof,

$$\begin{aligned}\sum_{i=0}^{k-2} \binom{n-1}{i} &= \sum_{i=0}^{k-2} \left[\binom{n-2}{i} + \binom{n-2}{i-1}\right] \\ &= \sum_{i=0}^{k-2} \binom{n-2}{i} + \sum_{i=0}^{k-3} \binom{n-2}{i} \\ &= \sum_{j=0}^{1} \binom{1}{j} \sum_{i=0}^{k-2-j} \binom{n-2}{i}\end{aligned}$$

Theorem 1: For any natural number n, m and k, 0≤k<n, 0≤m<k-2

$$\sum_{i=0}^{k-2} \binom{n-1}{i} = \sum_{j=0}^{m} \binom{m}{j} \sum_{i=0}^{k-2-j} \binom{n-m-1}{i}$$

Proof, we use the induction to prove the theorem. There is only one induction on m. If m = 0, then the equation is obviously right. If m = 1, then Lemma 3 provides the base case.

Next the induction hypothesis was made that the equation is right for if m, m+1,

$$\begin{aligned}&\sum_{j=0}^{m+1} \binom{m+1}{j} \sum_{i=0}^{k-2-j} \binom{n-(m+1)-1}{i} \\ &= \sum_{j=0}^{m+1} \left[\binom{m}{j} + \binom{m}{j-1}\right] \sum_{i=0}^{k-2-j} \binom{n-(m+1)-1}{i} \\ &= \sum_{j=0}^{m+1} \binom{m}{j} \sum_{i=0}^{k-2-j} \binom{n-(m+1)-1}{i} \\ &+ \sum_{j=0}^{m+1} \binom{m}{j-1} \sum_{i=0}^{k-2-j} \binom{n-(m+1)-1}{i} \\ &= \sum_{j=0}^{m} \binom{m}{j} \sum_{i=0}^{k-2-j} \binom{n-(m+1)-1}{i} \\ &+ \sum_{j=0}^{m} \binom{m}{j} \sum_{i=0}^{k-2-(j+1)} \binom{n-(m+1)-1}{i} \\ &= \sum_{j=0}^{m} \binom{m}{j} \sum_{i=0}^{k-2-j} \binom{n-(m+1)-1}{i} \\ &+ \sum_{j=0}^{m} \binom{m}{j} \sum_{i=0}^{k-2-j} \binom{n-(m+1)-1}{i-1} \\ &= \sum_{j=0}^{m} \binom{m}{j} \sum_{i=0}^{k-2-j} \left[\binom{n-m-2}{i} + \binom{n-m-2}{i-1}\right] \\ &= \sum_{j=0}^{m} \binom{m}{j} \sum_{i=0}^{k-2-j} \binom{n-m-1}{i} = \sum_{i=0}^{k-2} \binom{n-1}{i}\end{aligned}$$

So the theorem is proved.

CONSTRUCTION

In this subsection, we show the general construction of balanced algebraic immunity Boolean functions with Lobanov's nonliearity bound. The construction is listed below:

Construction: For any n and any,

$$k \le \left\lceil \frac{n}{2} \right\rceil$$

m is an odd number >n-2k, define the function $f_{n,k}$ by the next way:

$$f_{n,k}(x_1,\cdots,x_n) = \begin{cases} 0, & \text{if } wt(x_1,\cdots,x_n) < k \\ 1, & \text{if } wt(x_1,\cdots,x_n) > n-k \\ \sum_{i=1}^{m} x_i & \text{if } k \le wt(x_1,\cdots,x_n) \le n-k \end{cases}$$

If m = 1 then it is Lobanov (2005)'s construction

Theorem 2: The functions constructed with the above construction are balanced, Al ($f_{n,k}(x_1,...,x_n)$ = k and achieve Lobanov's bound. Proof, Note that f (x_1+1,...,x_n+1) = f (x_1+1,...,x_n+1), i.e., $f_{n,k}$ is a self-dual function. Hence, the function $f_{n,k}$ is a balanced function.

Since $f_{n,k}$ is self-dual in order to prove Al ($f_{n,k}$)≥, k, it is sufficient to prove that $f_{n,k}$+1 has not a nonzero annihilator of degree <k.

Write the possible annihilator g of the function f+1 of degree at most k-1 by means of indeterminate coefficients:

$$g = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1\le i\le j\le n} a_{ij} x_i x_j + \cdots + \sum_{1\le i_1\le\cdots\le i_{k-1}\le n} a_{i_1\cdots i_{k-1}} x_{i_1}\cdots x_{i_{k-1}}.$$

The function g is the annihilator of $f_{n,k}$+1 if and only if $f_{n,k}$+1 = 1 follows g (x). We obtain the system of homogeneous linear equations on the coefficients of the functions g: g (x_1...,x_n) for all vectors x such that wt (x)≤k-1.

Since g (0,...,0) = 0, we have α_0 = 0. Since g (x) if wt (x) = 1, we have a_1...a_0 = 0. Applying the induction on the weight of vectors we obtain that all coefficients of g are zeros. Hence, g (x) = 0. Thus, Al ($f_{n,k}$)≥k. At the same time it is easy to see that g (x_1...,x_n) = (x_1+1)...(x_1+1) is the annihilator of $f_{n,k}$ of degree k. Therefore Al ($f_{n,k}$) = k,. Calculate the Walsh coefficient of the function $f_{n,k}$ at the vector (1,0,...,0) using the self-duality off$_{n,k}$:

$$\begin{aligned} W_{f_{n,k}}(1,0,\cdots,0) &= \sum_{(x_1,\cdots,x_n)\in F_2^n} (-1)^{f_{n,k}(x_1,\cdots,x_n)+x_1} \\ &= 2^n - 2wt(f_{n,k}(x_1,\cdots,x_n)+x_1) \\ &= 2^n - 2[wt(f_{n,k}(0,x_2,\cdots,x_n)) \\ &\quad + wt(f_{n,k}(1,x_2,\cdots,x_n)+1)] \\ &= 2^n - 2\left[\sum_{j=0}^{m}\binom{m}{j}\sum_{i=n-k+1-(m-j)}^{n-m-1}\binom{n-m-1}{i} \right. \\ &\quad \left. + \sum_{j=0}^{m}\binom{m}{j}\sum_{i=0}^{k-2-j}\binom{n-m-1}{i}\right] \\ &= 2^n - 4\sum_{j=0}^{m}\binom{m}{j}\sum_{i=0}^{k-2-j}\binom{n-m-1}{i} \\ &= 2^n - 4\sum_{i=0}^{k-2}\binom{n-1}{i} \\ &= 2\sum_{i=k-1}^{n-k}\binom{n-1}{i} \end{aligned}$$

Hence, from Lemma 1, it get:

$$nl(f_{n,k}) = 2^{n-1} - \sum_{i=k-1}^{n-k}\binom{n-1}{i}$$

Count: Use the construction for any odd m >n-2k, it can get (n, m) balanced algebraic immune functions with Lobanov's bound, so: a lower bound of the count of these functions. As far as was got, this is the first bound about this count.

Theorem 3: The count of balanced algebraic immune functions with Lobanov's bound satisfied is more than:

$$\sum_{i=1,\,i\,\text{odd}}^{n-2k}\binom{n}{i}$$

CONCLUSION

In this correspondence, a general construction of balanced algebraic immunity Boolean function was given which has the tight nonlinearity bound proved by Lobanov and firstly gave a bound of these functions. It is interesting to study whether there are other constructions of these algebraic immunity Boolean functions.

REFERENCES

Carlet, C, D.K. Dalai, K.C. Gupta and S. Maitra, 2006. Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction. IEEE Trans. Inform. Theory, 57: 3105-3121.

Courtois, N. and W. Meier, 2002. Algebraic attacks on stream ciphers with linear feedback. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, May 4-8, Warsaw, pp: 346-359.

Dalai, D.K., K.C. Gupta and S. Maitra, 2004b. Cryptographically Significant Boolean Functions: Construction and Analysis in Terms of Algebraic Immunity, in FSE 2004 LNCS. Springer-Verlag, Berlin, Germany, pp: 98-111.

Dalai, K.D., K. C. Gupta and S. Maitra, 2004a. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions, in INDOCRYPT2004 LNCS. Springer-Verlag, Berlin, Germany, pp: 92-106.

Lobanov, M., 2005. Tight bound between nonlinearity and algebraic immunity. Cryptology ePrint Archive: Report 2005/441, http://eprint.iacr.org/2005/441.