International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.111-122
http://dx.doi.org/10.14257/ijsia.2015.9.2.11

A Proof of Constructions for Balanced Boolean Function with Optimum Algebraic Immunity

Yindong Chen, Wei Tian and Ya-nan Zhang

College of Engineering, Shantou University, Shantou, China
ydchen@stu.edu.cn

Abstract

Algebraic immunity is a cryptographic criterion for Boolean functions used in cryptosystem to resist algebraic attacks. They usually should have high algebraic immunity. Chen proposed a first order recursive construction of Boolean functions and checked that they had optimum algebraic immunity for n<8.This paper gives a detail proof of having optimum algebraic and being balanced for all n>0.

Keywords: *stream cipher, algebraic attacks, Boolean function, algebraic immunity*

1. Introduction

Recently, algebraic attack has gained a lot of attentions in cryptanalysis [1-4]. The main idea of algebraic attack is to deduce the security of a stream cipher to solving an over-defined system of multivariate nonlinear equations.

To resist algebraic attack, a new cryptographic property of Boolean functions, which is known as **algebraic immunity** (AI), has been proposed by Meier *et al.* [2]. Thus the AI of Boolean function used in cryptosystem should be sufficiently high. Courtois and Meier [1,2] showed that, for any *n*-variable Boolean function, its AI is upper bounded by $\lceil \frac{n}{2} \rceil$. If the bound is achieved, we say the Boolean function have optimum AI. Obviously, a Boolean function with optimum AI has strongest ability to resist standard algebraic attack. Therefore, the construction of Boolean functions with optimum AI is of great importance.

Dalai [5-6] presented Boolean functions with optimum AI in even variables by a recursive construction for the first time. It's a second order recursive construction. However, further study [5] showed that the functions are not balanced. Another class of constructions [7-8] contains symmetric functions. Being symmetric, they present a risk if attacks using this peculiarity can be found in the future. Moreover, they do not have high nonlinearity [9]. Li [10] proposed a method to construct all (2*k*+1)-variable Boolean functions with optimum AI from one such given function. But the computational complexity of the construction do not have been well studied. Carlet and Feng [11] proposed a well construction based on the Boolean functions' trace representation. Their Boolean functions have not only optimum AI but also high nonlinearity. Furthermore, they also have a good behavior against fast algebraic attacks, at least for small values of the number of variables. The drawback of the construction is the high complexity of the computation for the value of $f(x)$. Chen [12] presented a new category of even-variable rotation symmetric Boolean functions with optimum AI, in which there are altogether $\lfloor \frac{n}{4} \rfloor - 3$ different constructions. They also showed that the constructed Boolean functions had high nonlinearity.

Different with Dalai's second order recursive construction, Chen [13] proposed a first order recursive construction. Furthermore, the constructed Boolean functions are balanced.

ISSN: 1738-9976 IJSIA

But there is no proofs. They only checked for $1 \le n \le 6$ that the constructed Boolean functions are balanced and have optimum AI. In the following, we will prove in detail that ϕ_n is balanced and has optimum AI for all n.

The organization of the paper is as follows. In the following section we give some preliminaries about Boolean functions. In Section 3, we present a detail proof of the constructed Boolean functions to have optimum AI. In Section 4, their cryptographic properties are studied. Section 5 concludes the paper.

2. Preliminaries

2.1. Boolean Function

Denote $\mathbf{F}_2=\{0,1\}$, the finite field with two elements. Then a Boolean function in n variables is defined as mapping from $\mathbf{F}_2^n$ into $\mathbf{F}_2$. Denote by B_n the set of all n-variable Boolean functions. A basic representation of a Boolean function $f(x_1,\ldots,x_n)$ is by the output column of its truth table, i.e., a binary string of length 2^n.

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

For each n-variables Boolean function f, we define its **support** and **offset** as

$$\begin{cases} \mathrm{supp}(f) = \{X \in \mathrm{F}_2^n \mid f(X) = 1\}, \\ \mathrm{offset}(f) = \{X \in \mathrm{F}_2^n \mid f(X) = 0\}, \end{cases}$$

The **Hamming weight** wt(f) of f is the size of supp(f), i.e., wt(f)=|supp(f)|. It counts the number of 1's in the truth table of f. We say f is **balanced**, if the truth table contains an equal number of 1's and 0's, *i.e.*, |supp(f)|=|offset(f)|, implying wt(f)=2^{n-1}.

Each Boolean function has another unique representation as a multivariate polynomial over $\mathbf{F}_2$, called the **algebraic normal form** (ANF):

$$f(X_1, X_2, \cdots, X_n) = a_0 + \sum_{1 \le i \le n} a_i X_i + \sum_{1 \le i < j \le n} a_{i,j} X_i X_j + \cdots + a_{1,2,\ldots,n} X_1 X_2 \cdots X_n,$$

where the coefficients $a_0, a_i, a_{ij}, \ldots, a_{12\ldots n} \in \mathbf{F}_2$.

The **algebraic degree** deg(f) of f is the number of variables in the highest order term with nonzero coefficient.

2.2. Algebraic Immunity of Boolean function

Definition 1. Given $f \in B_n$, we define

$$\mathrm{Ann}(f) = \{g \in B_n \mid g \cdot f = 0\}$$

Any function $g \in \mathrm{Ann}(f)$ is called an annihilator of f.

Definition 2. Given $f \in B_n$, we define its algebraic immunity, denote by AI(f), as the minimum degree of all nonzero annihilators of f or f+1, i.e.,

$$\mathrm{AI}(f) = \min\{\deg(g) \mid 0 \ne g \in \mathrm{Ann}(f) \cup \mathrm{Ann}(f+1)\}$$

For $f \in B_n$, it has been proved that $\mathrm{AI}(f) \le \lceil \frac{n}{2} \rceil$ [2]. If $\mathrm{AI}(f) = \lceil \frac{n}{2} \rceil$, we say it has optimum AI. The AI of a Boolean function expresses its ability to resist standard algebraic attack. So, Boolean functions with higher AI (even optimum AI) is preferred in cryptosystem.

2.3. The Concatenation Operation of Boolean Function

We can use a binary string of length 2^n to express an n-variable Boolean function, and denote by "||" the concatenation of binary strings.

Proposition 1. For $\forall f = f_1 \| f_2$, where $f_1, f_2 \in B_n$, there is

i) $f \in B_{n+1}$ and $f = f_1 + x_{n+1}(f_1+f_2)$;

ii) for $\forall g \in \mathrm{Ann}(f)$, decompose it as $g = g_1 \| g_2$, where $g_1, g_2 \in B_{n-1}$, then $g_1 \in \mathrm{Ann}(f_1)$ and $g_2 \in \mathrm{Ann}(f_2)$.

3. A Recursive Construction of Boolean Function with Optimum Algebraic Immunity

For any Boolean function f, we denote $\bar{f}$ the complement Boolean function of f, *i.e.*, $\bar{f} = f+1$.

Now, we're proposing a first order recursive construction of Boolean function, and then proving that they have optimum AI.

Construction 1.

$$\begin{cases} \phi_{n+1} = \phi_n \| \bar{\phi}_n^1, \\ \phi_{n+1}^i = \phi_n^{i-1} \| \bar{\phi}_n^{i+1}, \end{cases} \tag{1}$$

with base step $\phi_n^0 = \phi_n$, $\phi_1^j = x_1 + 1 + (j \bmod 2)$, where $i, n \geq 1$, $j \geq 0$.

In [13], we proposed the upper construction, and checked that the constructed Boolean functions ϕ_n is balanced and has optimum AI for $1 \leq n \leq 6$. In the following, we will prove in detail that ϕ_n is balanced and has optimum AI for all n.

For convenience in description, we define $\phi_n^{-1} = \phi_n^0 = \phi_n$, then the upper recursion can be simplified as

$$\phi_{n+1}^i = \phi_n^{i-1} \| \bar{\phi}_n^{i+1}. \tag{2}$$

To prove that ϕ_n has optimum AI, we need intermediate results. For technical reasons, during our proofs, we will encounter certain situations when the degree of a function is negative. As such functions do not exist, we will replace them by function 0.

Lemma 1. Assume the function $\phi_n \in B_n$ has been generated by Construction 1 and $\mathrm{AI}(\phi_t) = \lceil \frac{t}{2} \rceil$ for $1 \leq t \leq n$. If there exists

i) $g \in \mathrm{Ann}(\phi_n^i), h \in \mathrm{Ann}(\bar{\phi}_n^{i+1})$, or

ii) $g \in \mathrm{Ann}(\bar{\phi}_n^i), h \in \mathrm{Ann}(\phi_n^{i+1})$,

such that $\deg(g+h) \leq \lfloor \frac{n-i}{2} \rfloor - 1$ and $i \geq 0$, then

$$g = h.$$

Proof. We prove it by induction on n.

For the base step $n = 1$, it can be easily checked. Now we prove the induction step.

Assume that the induction assumption holds for all $n < k$, we are to prove it for $n = k$.

i) Suppose $g \in \mathrm{Ann}(\phi_k^i), h \in \mathrm{Ann}(\bar{\phi}_k^{i+1})$, such that $\deg(g+h) \leq \lfloor \frac{k-i}{2} \rfloor - 1$ and $i \geq 0$.

Decompose g, h as

$$\begin{cases} g = g_1 \| g_2, \\ h = h_1 \| h_2, \end{cases}$$

where $g_1, g_2, h_1, h_2 \in B_{k-1}$.

By Recursion (2), we have

$$\begin{cases} \phi_k^i = \phi_{k-1}^{i-1} \| \bar{\phi}_{k-1}^{i+1}, \\ \bar{\phi}_k^{i+1} = \bar{\phi}_{k-1}^{i} \| \phi_{k-1}^{i+2}. \end{cases}$$

According to Proposition 1, there is

$$\begin{aligned} g+h &= \left(g_1 + X_k(g_1+g_2)\right) + \left(h_1 + X_k(h_1+h_2)\right) \\ &= (g_1+h_1) + X_k(g_1+g_2+h_1+h_2), \end{aligned} \tag{3}$$

and

$$\begin{cases} g_1 \in \mathrm{Ann}(\phi_{k-1}^{i-1}), \\ g_2 \in \mathrm{Ann}(\overline{\phi}_{k-1}^{i+1}), \\ h_1 \in \mathrm{Ann}(\overline{\phi}_{k-1}^{i}), \\ h_2 \in \mathrm{Ann}(\phi_{k-1}^{i+2}). \end{cases} \tag{4}$$

a) To prove $g_1 = h_1$.

According to (3),

$$\begin{aligned} \deg(g_1+h_1) &\le \deg(g+h) \\ &\le \left\lfloor \tfrac{k-i}{2} \right\rfloor - 1 \\ &= \left\lfloor \tfrac{(k-1)-(i-1)}{2} \right\rfloor - 1. \end{aligned}$$

According to (4), there is

$$\begin{cases} g_1 \in \mathrm{Ann}(\phi_{k-1}^{i-1}), \\ h_1 \in \mathrm{Ann}(\overline{\phi}_{k-1}^{i}). \end{cases}$$

By induction assumption, thus

$$g_1 = h_1.$$

b) To prove $g_2 = h_2$.

Since $g_1 = h_1$, (3) changes into

$$\begin{aligned} g+h &= (g_1+h_1) + X_k(g_1+g_2+h_1+h_2) \\ &= X_k(g_2+h_2), \end{aligned}$$

Then,

$$\begin{aligned} \deg(g_2+h_2) &= \deg(g+h) - 1 \\ &\le \left(\left\lfloor \tfrac{k-i}{2} \right\rfloor - 1\right) - 1 \\ &= \left\lfloor \tfrac{(k-1)-(i+1)}{2} \right\rfloor - 1. \end{aligned}$$

According to (4), there is

$$\begin{cases} g_2 \in \mathrm{Ann}(\overline{\phi}_{k-1}^{i+1}), \\ h_2 \in \mathrm{Ann}(\phi_{k-1}^{(i+1)+1}). \end{cases}$$

By induction assumption, thus

$$g_2 = h_2.$$

Hence we get $g+h=0$, i.e.,

$$g = h.$$

ii) Suppose $g \in \mathrm{Ann}(\overline{\phi}_n^{i}),\ h \in \mathrm{Ann}(\phi_n^{i+1}),$ such that $\deg(g+h) \le \left\lfloor \tfrac{k-i}{2} \right\rfloor - 1$ and $i \ge 0$.

Decompose g, h as

$$\begin{cases} g = g_1 \,\|\, g_2, \\ h = h_1 \,\|\, h_2, \end{cases}$$

where $g_1, g_2, h_1, h_2 \in \mathrm{B}_{k-1}$.

By Recursion (2), we have

$$\begin{cases} \overline{\phi}_k^i = \overline{\phi}_{k-1}^{i-1} \| \phi_{k-1}^{i+1}, \\ \phi_k^{i+1} = \phi_{k-1}^i \| \overline{\phi}_{k-1}^{i+2}. \end{cases}$$

According to Proposition 1, there is

$$\begin{aligned} g+h &= \left(g_1 + X_k(g_1+g_2)\right) + \left(h_1 + X_k(h_1+h_2)\right) \\ &= (g_1+h_1) + X_k(g_1+g_2+h_1+h_2), \end{aligned} \tag{5}$$

and

$$\begin{cases} g_1 \in \mathrm{Ann}(\overline{\phi}_{k-1}^{i-1}), \\ g_2 \in \mathrm{Ann}(\phi_{k-1}^{i+1}), \\ h_1 \in \mathrm{Ann}(\phi_{k-1}^{i}), \\ h_2 \in \mathrm{Ann}(\overline{\phi}_{k-1}^{i+2}). \end{cases} \tag{6}$$

a) To prove $g_1 = h_1$.

According to (5),

$$\begin{aligned} \deg(g_1+h_1) &\le \deg(g+h) \\ &\le \left\lfloor \tfrac{k-i}{2} \right\rfloor - 1 \\ &= \left\lfloor \tfrac{(k-1)-(i-1)}{2} \right\rfloor - 1. \end{aligned}$$

According to (6), there is

$$\begin{cases} g_1 \in \mathrm{Ann}(\overline{\phi}_{k-1}^{i-1}), \\ h_1 \in \mathrm{Ann}(\phi_{k-1}^{i}). \end{cases}$$

By induction assumption, thus

$$g_1 = h_1.$$

b) To prove $g_2 = h_2$.

Since $g_1 = h_1$, (5) changes into

$$\begin{aligned} g+h &= (g_1+h_1) + X_k(g_1+g_2+h_1+h_2) \\ &= X_k(g_2+h_2), \end{aligned}$$

Then,

$$\begin{aligned} \deg(g_2+h_2) &= \deg(g+h) - 1 \\ &\le \left(\left\lfloor \tfrac{k-i}{2} \right\rfloor - 1\right) - 1 \\ &= \left\lfloor \tfrac{(k-1)-(i+1)}{2} \right\rfloor - 1. \end{aligned}$$

According to (6), there is

$$\begin{cases} g_2 \in \mathrm{Ann}(\phi_{k-1}^{i+1}), \\ h_2 \in \mathrm{Ann}(\overline{\phi}_{k-1}^{(i+1)+1}). \end{cases}$$

By induction assumption, thus

$$g_2 = h_2.$$

Hence we get $g+h=0$, i.e.,

$$g = h.$$

Summing up i) and ii), the lemma is proved.

Lemma 2. Assume that the function $\phi_n \in \mathrm{B}_n$ has been generated by Construction 1 and $\mathrm{AI}(\phi_t) = \lceil \tfrac{n}{2} \rceil$ for $1 \le t \le n$. If there exists

i) $g \in \mathrm{Ann}(\phi_n^i) \bigcap \mathrm{Ann}(\overline{\phi}_n^{i+1})$, or

ii) $g \in \mathrm{Ann}(\bar{\phi}_n^i) \bigcap \mathrm{Ann}(\phi_n^{i+1})$,

such that $\deg(g) \le \left\lfloor \frac{n+i}{2} \right\rfloor$ and $i \ge 0$, then

$$g = 0.$$

Proof. We prove the lemma by induction on *n*.

For the base step $n = 1$, it can be easily checked. Now we prove the induction step.

Assume that the induction assumption holds for all $n < k$, we are to prove it for $n = k$.

i) Suppose $g \in \mathrm{Ann}(\phi_n^i) \bigcap \mathrm{Ann}(\bar{\phi}_n^{i+1})$, such that $\deg(g) \le \left\lfloor \frac{n+i}{2} \right\rfloor$ and $i \ge 0$.

Decompose g as

$$g = g_1 \| g_2,$$

where $g_1, g_2 \in \mathrm{B}_{k-1}$.

By Recursion (2), we have

$$\begin{cases} \phi_k^i = \phi_{k-1}^{i-1} \| \bar{\phi}_{k-1}^{i+1}, \\ \bar{\phi}_k^{i+1} = \bar{\phi}_{k-1}^{i} \| \phi_{k-1}^{i+2}. \end{cases}$$

According to Proposition 1, there is

$$g = g_1 + X_k(g_1 + g_2), \tag{7}$$

and,

$$\begin{cases} g_1 \in \mathrm{Ann}(\phi_{k-1}^{i-1}), \\ g_2 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i+1}), \\ g_1 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i}), \\ g_2 \in \mathrm{Ann}(\phi_{k-1}^{i+2}), \end{cases} \tag{8}$$

a) To prove $g_2 = 0$.

According to (7),

$$\begin{aligned} \deg(g_2) &\le \deg(g) \\ &\le \left\lfloor \frac{k+i}{2} \right\rfloor \\ &= \left\lfloor \frac{(k-1)+(i+1)}{2} \right\rfloor. \end{aligned}$$

According to (8), there is

$$\begin{cases} g_2 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i+1}), \\ g_2 \in \mathrm{Ann}(\phi_{k-1}^{i+2}), \end{cases}$$

i.e., $g_2 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i+1}) \bigcap \mathrm{Ann}(\phi_{k-1}^{(i+1)+1})$.

By induction assumption, thus

$$g_2 = 0.$$

b) To prove $g_1 = 0$.

Since $g_2 = 0$, (7) changes into

$$\begin{aligned} g &= g_1 + X_k(g_1 + g_2) \\ &= (1 + X_k)g_1, \end{aligned}$$

Then,

$$\begin{aligned} \deg(g_1) &= \deg(g) - 1 \\ &\le \left\lfloor \frac{k+i}{2} \right\rfloor - 1 \\ &= \left\lfloor \frac{(k-1)+(i-1)}{2} \right\rfloor. \end{aligned}$$

According to (8), there is

$$\begin{cases} g_1 \in \mathrm{Ann}(\phi_{k-1}^{i-1}), \\ g_1 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i}), \end{cases}$$

i.e., $g_1 \in \mathrm{Ann}(\phi_{k-1}^{i-1}) \bigcap \mathrm{Ann}(\bar{\phi}_{k-1}^{(i-1)+1})$.

By induction assumption, thus

$$g_1 = 0.$$

Hence we get

$$g = 0.$$

ii) Suppose $g \in \mathrm{Ann}(\bar{\phi}_n^{i}) \bigcap \mathrm{Ann}(\phi_n^{i+1})$, such that $\deg(g) \le \left\lfloor \frac{n+i}{2} \right\rfloor$ and $i \ge 0$.

Decompose g as

$$g = g_1 \| g_2,$$

where $g_1, g_2 \in \mathrm{B}_{k-1}$.

By Recursion (2), we have

$$\begin{cases} \bar{\phi}_k^{i} = \bar{\phi}_{k-1}^{i-1} \| \phi_{k-1}^{i+1}, \\ \phi_k^{i+1} = \phi_{k-1}^{i} \| \bar{\phi}_{k-1}^{i+2}. \end{cases}$$

According to Proposition 1, there is

$$g = g_1 + X_k(g_1 + g_2), \tag{9}$$

and,

$$\begin{cases} g_1 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i-1}), \\ g_2 \in \mathrm{Ann}(\phi_{k-1}^{i+1}), \\ g_1 \in \mathrm{Ann}(\phi_{k-1}^{i}), \\ g_2 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i+2}), \end{cases} \tag{10}$$

a) To prove $g_2 = 0$.

According to (9),

$$\begin{aligned} \deg(g_2) &\le \deg(g) \\ &\le \left\lfloor \frac{k+i}{2} \right\rfloor \\ &= \left\lfloor \frac{(k-1)+(i+1)}{2} \right\rfloor. \end{aligned}$$

According to (10), there is

$$\begin{cases} g_2 \in \mathrm{Ann}(\phi_{k-1}^{i+1}), \\ g_2 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i+2}), \end{cases}$$

i.e., $g_2 \in \mathrm{Ann}(\phi_{k-1}^{i+1}) \bigcap \mathrm{Ann}(\bar{\phi}_{k-1}^{(i+1)+1})$.

By induction assumption, thus

$$g_2 = 0.$$

b) To prove $g_1 = 0$.

Since $g_2 = 0$, (9) changes into

$$\begin{aligned} g &= g_1 + X_k(g_1 + g_2) \\ &= (1 + X_k)g_1, \end{aligned}$$

Then,

$$\begin{aligned} \deg(g_1) &= \deg(g) - 1 \\ &\le \left\lfloor \frac{k+i}{2} \right\rfloor - 1 \\ &= \left\lfloor \frac{(k-1)+(i-1)}{2} \right\rfloor. \end{aligned}$$

According to (10), there is

$$\begin{cases} g_1 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i-1}), \\ g_1 \in \mathrm{Ann}(\phi_{k-1}^{i}), \end{cases}$$

i.e., $g_1 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{i-1}) \bigcap \mathrm{Ann}(\phi_{k-1}^{(i-1)+1})$.

By induction assumption, thus

$$g_1 = 0 .$$

Hence we get

$$g = 0 .$$

Summing up i) and ii), the lemma is proved.

Theorem 1. For every $n \geq 1$, the function ϕ_n obtained in Construction 1 has optimum algebraic immunity, *i.e.*

$$\mathrm{AI}(\phi_n) = \left\lceil \frac{n}{2} \right\rceil .$$

Proof. We prove the Theorem by induction on *n*.

For the base step $n = 1$, it can be easily checked. Now we prove the induction step.

Assume that the induction assumption holds for all $n < k$, we are to prove it for $n = k$.

It just need to prove that for $\forall g \in \mathrm{Ann}(\phi_k) \bigcup \mathrm{Ann}(\phi_k + 1)$, if $\deg(g) < \left\lceil \frac{k}{2} \right\rceil$, there should be $g = 0$.

1) Suppose $g \in \mathrm{Ann}(\phi_k)$.

Decompose g as

$$g = g_1 \| g_2,$$

where $g_1, g_2 \in \mathrm{B}_{k-1}$.

By Recursion (1) we have

$$\phi_k = \phi_{k-1} \| \bar{\phi}_{k-1}^{1} .$$

According to Proposition 1, there is

$$g = g_1 + x_k(g_1 + g_2), \tag{11}$$

and,

$$\begin{cases} g_1 \in \mathrm{Ann}(\phi_{k-1}), \\ g_2 \in \mathrm{Ann}(\bar{\phi}_{k-1}^{1}). \end{cases} \tag{12}$$

According to (11),

$$\begin{aligned} \deg(g_1 + g_2) &\leq \deg(g) - 1 \\ &< \left\lceil \frac{k}{2} \right\rceil - 1 \\ &= \left\lfloor \frac{k-1}{2} \right\rfloor \\ &\leq \left\lfloor \frac{k-1}{2} \right\rfloor - 1. \end{aligned}$$

According to Lemma 1,

$$g_1 = g_2 .$$

Then (12) and (11) change into

$$g_1 \in \mathrm{Ann}(\phi_{k-1}) \bigcap \mathrm{Ann}(\bar{\phi}_{k-1}^{1}),$$

and

$$g = g_1.$$

Thus,

$$\begin{aligned}\deg(g_1) &= \deg(g)\\ &< \left\lceil \tfrac{k}{2} \right\rceil\\ &\le \left\lceil \tfrac{k}{2} \right\rceil - 1\\ &= \left\lfloor \tfrac{k-1}{2} \right\rfloor.\end{aligned}$$

According to Lemma 2,

$$g_1 = 0.$$

Hence,

$$g = 0.$$

2) Suppose $g \in \mathrm{Ann}(\phi_k + 1)$, i.e., $g \in \mathrm{Ann}(\bar{\phi}_k)$.

Decompose g as

$$g = g_1 \| g_2,$$

where $g_1, g_2 \in \mathrm{B}_{k-1}$.

By Recursion (1) we have

$$\bar{\phi}_k = \bar{\phi}_{k-1} \| \phi_{k-1}^1.$$

According to Proposition 1, there is

$$g = g_1 + X_k(g_1 + g_2), \tag{13}$$

and

$$\begin{cases} g_1 \in \mathrm{Ann}(\bar{\phi}_{k-1}), \\ g_2 \in \mathrm{Ann}(\phi_{k-1}^1). \end{cases} \tag{14}$$

According to (13),

$$\begin{aligned}\deg(g_1 + g_2) &\le \deg(g) - 1\\ &< \left\lceil \tfrac{k}{2} \right\rceil - 1\\ &= \left\lfloor \tfrac{k-1}{2} \right\rfloor\\ &\le \left\lfloor \tfrac{k-1}{2} \right\rfloor - 1.\end{aligned}$$

According to Lemma 1,

$$g_1 = g_2.$$

Then (14) and (13) change into

$$g_1 \in \mathrm{Ann}(\bar{\phi}_{k-1}) \bigcap \mathrm{Ann}(\phi_{k-1}^1),$$

and

$$g = g_1.$$

Thus,

$$\begin{aligned}\deg(g_1) &= \deg(g)\\ &< \left\lceil \tfrac{k}{2} \right\rceil\\ &\le \left\lceil \tfrac{k}{2} \right\rceil - 1\\ &= \left\lfloor \tfrac{k-1}{2} \right\rfloor.\end{aligned}$$

According to Lemma 2,

$$g_1 = 0.$$

Hence,

$$g = 0.$$

Summing up 1) and 2), for $\forall g \in \mathrm{Ann}(\phi_k) \bigcup \mathrm{Ann}(\phi_k + 1)$, if $\deg(g) < \left\lceil \tfrac{k}{2} \right\rceil$, there should be $g = 0$. Therefore,

$$\mathrm{AI}(\phi_n) = \left\lceil \frac{n}{2} \right\rceil.$$

4. Other Cryptographic Properties

In this section, we are going to show that the constructed Boolean functions are all balanced.

Property 1. The Boolean function ϕ_n^i and $\bar{\phi}_n^i$ $(n \geq 1, i \geq 0)$ obtained in Construction 1 are both balanced.

Proof. We prove it by induction on *n*.

For n=1, we have

$$\phi_1^i = \begin{cases} 10, & i \text{ odd;} \\ 01, & i \text{ even.} \end{cases}$$

and

$$\bar{\phi}_1^i = \begin{cases} 01, & i \text{ odd;} \\ 10, & i \text{ even.} \end{cases}$$

It's obviously that ϕ_1^i and $\bar{\phi}_1^i$ are both balanced.

Suppose that the statement holds for $n < k$, we show it for $n = k$.

i) For $i > 0$, there's i-1, i+1 ≥ 0.

According to Recursion (1),

$$\begin{cases} \phi_k^i = \phi_{k-1}^{i-1} \| \bar{\phi}_{k-1}^{i+1}, \\ \bar{\phi}_k^i = \bar{\phi}_{k-1}^{i-1} \| \phi_{k-1}^{i+1}, \end{cases}$$

By induction assumption $\phi_{k-1}^{i-1}, \bar{\phi}_{k-1}^{i+1}, \bar{\phi}_{k-1}^{i-1}$ and ϕ_{k-1}^{i+1} are all balanced.

Then,

$$\mathrm{wt}(\phi_{k-1}^{i-1}) = \mathrm{wt}(\bar{\phi}_{k-1}^{i+1}) = \mathrm{wt}(\bar{\phi}_{k-1}^{i-1}) = \mathrm{wt}(\phi_{k-1}^{i+1}) = 2^{k-2}.$$

Thus,

$$\begin{cases} \mathrm{wt}(\phi_k^i) = \mathrm{wt}(\phi_{k-1}^{i-1}) + \mathrm{wt}(\bar{\phi}_{k-1}^{i+1}) = 2 \times 2^{k-2} = 2^{k-1}, \\ \mathrm{wt}(\bar{\phi}_k^i) = \mathrm{wt}(\bar{\phi}_{k-1}^{i-1}) + \mathrm{wt}(\phi_{k-1}^{i+1}) = 2 \times 2^{k-2} = 2^{k-1}, \end{cases}$$

i.e., ϕ_k^i and $\bar{\phi}_k^i$ are both balanced.

ii) For $i = 0$,

According to Recursion (1),

$$\begin{cases} \phi_k = \phi_{k-1} \| \bar{\phi}_{k-1}^1, \\ \bar{\phi}_k = \bar{\phi}_{k-1} \| \phi_{k-1}^1, \end{cases}$$

By induction assumption $\phi_{k-1}, \bar{\phi}_{k-1}^1, \bar{\phi}_{k-1}$ and ϕ_{k-1}^1 are all balanced.

Then,

$$\mathrm{wt}(\phi_{k-1}) = \mathrm{wt}(\bar{\phi}_{k-1}^1) = \mathrm{wt}(\bar{\phi}_{k-1}) = \mathrm{wt}(\phi_{k-1}^1) = 2^{k-2}.$$

Thus,

$$\begin{cases} \mathrm{wt}(\phi_k) = \mathrm{wt}(\phi_{k-1}) + \mathrm{wt}(\bar{\phi}_{k-1}^1) = 2 \times 2^{k-2} = 2^{k-1}, \\ \mathrm{wt}(\bar{\phi}_k) = \mathrm{wt}(\bar{\phi}_{k-1}) + \mathrm{wt}(\phi_{k-1}^1) = 2 \times 2^{k-2} = 2^{k-1}, \end{cases}$$

i.e., ϕ_k and $\bar{\phi}_k$ are both balanced.

Therefore, ϕ_k^i and $\bar{\phi}_k^i$ $(i \geq 0)$ are both balanced. And according to induction principle, the Boolean function ϕ_n^i and $\bar{\phi}_n^i$ $(n \geq 1, i \geq 0)$ obtained in Construction 1 are all balanced.

From Property 1, we can directly get the following corollary.

Corollary 1. The Boolean function ϕ_n^i $(n \geq 1, i \geq 0)$ obtained in Construction 1 is balanced.

5. Conclusion

In this paper, we proposed a first order recursive construction of Boolean function with optimum algebraic immunity. We made a quite detail proof that they not only had optimum AI but also being balanced, which is a superiority of the constructed Boolean functions.

Acknowledgements

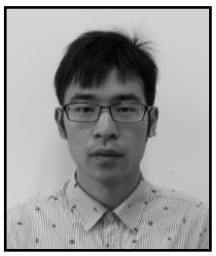
This paper is a revised and expanded version of a paper entitled "Construction for Balanced Boolean Function with Maximum Algebraic Immunity" presented at ASEA 2014, Haikou, China, 2014.This work was supported by the Natural Science Foundation of China (No.61103244), the Foundation for Distinguished Young Talents in Higher Education of Guangdong, China (No.LYM11064), the Excellent Young Teachers Program of Guangdong Higher Education (No.Yq2013074), the Engineering and Technology Research Center of Guangdong Higher Education Institutes(No.GCZX-A1306), and the Academic Innovation Team Construction Project of Shantou University (No.ITC12001)

References

[1] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback", Advances in Cryptology-EUROCRYPT 2003, LNCS, vol. 2656, **(2003)**, pp. 345-359.
[2] W. Meier, E. Pasalic and C. Carlet, "Algebraic attacks and decomposition of Boolean functions", Advances in Cryptology-EUROCRYPT 2004, LNCS, vol. 3027, **(2004)**, pp. 474-491.
[3] F. Armknecht and M. Krause, "Algebraic Attacks on Combiners with Memory", Advances in Cryptology-Crypto 2003[C], Berlin: Springer-Verlag, **(2003)**, pp. 162-175
[4] N. Courtois, "Cryptanalysis of SFINKS", Information Security and Cryptology—ICISC 2005, LNCS, vol. 3935, Springer-Verlag, **(2006)**, pp. 261-269.
[5] C. Carlet, D.K. Dalai, K. C. Gupta and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: analysis and construction", IEEE Transactions on Information Theory, vol. 52, **(2006)**, pp. 3105-3121.
[6] [6] D. K. Dalai, K. C. Gupta and S. Maitra. "Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity" Fast Software Encryption 2005 (FSE05) , Paris, France, **(2005)**, pp. 98-111
[7] A. Braeken and B. Preneel, "On the algebraic immunity of symmetric Boolean functions". Progress in Cryptology-Indocrypt 2005, Berlin: Springer-Verlag, **(2005)**, pp. 35-48
[8] C. Carlet, "A method of construction of balanced functions with optimum algebraic immunity", http://eprint.iacr.org/2006/149
[9] C. Carlet, X. Zeng and C. Li, "Further properties of several classes of Boolean functions with optimum algebraic immunity", http://eprint.iacr.org/2007/370
[10] N. Li and W. Qi, "Construction and analysis of Boolean functions of 2t+1 variables with maximum algebraic immunity", Advances in Cryptology-Asiacrypt 2006, Berlin: Springer-Verlag, **(2006)**, pp. 84-98
[11] C. Carlet and K. Feng, "An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity". Advances in Cryptology-Asiacrypt 2008, Berlin: Springer-Verlag, **(2008)**, pp. 425-440.
[12] Y. Chen, H. Xiang and Y. Zhang, "New construction of even-variable rotation symmetric Boolean functions with optimum algebraic immunity. International Journal of Security and its Applications", vol. 8, no. 1, **(2014)**, pp. 307-318.
[13] Y. Chen, W. Tian and Y. Zhang, "Construction for Balanced Boolean Function with Maximum Algebraic Immunity", The 2nd International Conference on Information Science and Technology, IST 2014, **(2014)**.

Authors

Yindong Chen, he received Ph.D. from the Fudan University in 2010. Currently he is an Associate Professor at Shantou University, China. His research interest is in Cryptology and Information Security.



Wei Tian, he is a postgraduate student at Shantou University, China. His research interest is in Cryptology and Information Security.

Ya-nan Zhang, he is a postgraduate student at Shantou University, China. His research interest is in Cryptology and Information Security.