International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.307-318
http://dx.doi.org/10.14257/ijsia.2014.8.1.29

New Construction of Even-variable Rotation Symmetric Boolean Functions with Optimum Algebraic Immunity

Yindong Chen*, Hongyan Xiang and Ya-nan Zhang

(College of Engineering, Shantou University, Shantou, 515063 China)
*(*ydchen@stu.edu.cn)*

Abstract

The rotation symmetric Boolean functions which are invariant under the action of cyclic group have been used as components of different cryptosystems. In order to resist algebraic attacks, Boolean functions should have high algebraic immunity. This paper studies the construction of even-variable rotation symmetric Boolean functions with optimum algebraic immunity. We construct $(\lfloor n/4 \rfloor - 3)$ *different rotation symmetric Boolean functions which achieve both optimum algebraic immunity and high nonlinearity when an even* n $(n \geq 16)$ *is given.*

Keywords: *Algebraic attacks, Rotation symmetric Boolean functions, Algebraic immunity*

1. Introduction

Boolean functions play an important role in some cryptosystems of stream ciphers. In order to resist different attacks to cryptosystems algorithms, a variety of properties for choosing Boolean functions should be considered such as balancedness, nonlinearity, algebraic degree, *etc*.

In recent years, algebraic attacks [1, 2] have become an important tool in cryptanalysis of stream ciphers, the main idea of which is to solve a system of low degree multivariate equations with unknown input keys. With this method, some cryptographic algorithms have been successfully attacked, such as Toyocrypt [3], LILI-128 [1], SFINKS [4] and so on. Then a new cryptographic property of Boolean functions called algebraic immunity(AI) has been introduced [5, 6]. In order to resist algebraic attacks, Boolean functions should have high AI. As is shown in [6], the AI of an n-variable Boolean functions is upper bounded by $\lceil n/2 \rceil$. If the bound is achieved, we say the Boolean function has optimum AI. Since 2003 several classes of Boolean functions with optimum AI have been investigated and constructed to withstand the algebraic attack [7-10, 18].

Rotation symmetric Boolean functions(RSBFs) [11] are invariant under the action of cyclic group which are good candidates with optimum AI. So far, many rotation symmetric Boolean functions with optimum AI have been obtained [12-17]. In 2007, Sarkar and Maitra [12] constructed odd-variables rotation symmetric Boolean functions with optimum AI and the nonlinearity of $2^{n-1} - \binom{n-1}{(n-1)/2} + 2$. Later in 2009, Sarkar *et al.*, [13] presented rotation symmetric Boolean functions on even-variable with optimum AI and nonlinearity higher than $2^{n-1} - \binom{n-1}{n/2} + 4$. In 2010, Meng *et al.*, [14] gave a construction of Boolean functions with optimum AI on even-variable. On the base of this method, they also gave a construction of balanced rotation symmetric Boolean functions with optimum AI on 2^m-variable. In 2011, Fu *et al.*, [15] presented balanced rotation symmetric Boolean functions with optimum AI which

ISSN: 1738-9976 IJSIA

has higher nonlinearity, but the construction was also just for 2^m-variable. In 2012, the first paper [16] showed a method of constructing rotation symmetric Boolean functions with optimum AI which had $\frac{n}{2}-1$ different functions in total by giving an even n. Fu *et al.*, [17] gave a construction of even-variable RSBFs with optimum AI and the very high nonlinearity in 2013. Especially, Su *et al.*, [18] presented two new kinds of construction of rotation symmetric Boolean functions having optimum AI on either odd variables or even variables. Furthermore, their new functions were of much better nonlinearity than all the existing construction. We propose a well construction which have $\lfloor n/4 \rfloor - 3$ different RSBFs by giving an even n ($n \geq 16$), and the nonlinearity of our construction is high enough.

The paper is organized as follows. Section 2 provides basic definitions and notations. In Section 3, a new construction of RSBFs on even-variables with optimum AI is given. The nonlinearity of constructed even-variable RSBFs is studied in Section 4. Section 5 concludes this paper.

2. Preliminaries

Denote $\mathrm{F}_2 = \{0,1\}$, the finite field with two elements. Then a Boolean function on n-variable can be viewed as a mapping from F_2^n to F_2. Let B_n be the set of all n-variable Boolean functions. For a vector $x = (x_1, x_2, ..., x_n) \in \mathrm{F}_2^n$, the support of x is denoted by $\mathrm{supp}(x)=\{\mathrm{i}|x_i=1, 1 \leq \mathrm{i} \leq n\}$, and the Hamming weight $\mathrm{wt}(x)$ of x is the cardinality of $\mathrm{supp}(x)$. Any Boolean function $f(x_1, x_2, ..., x_n)$ can be given by its truth table, which is a binary string of length 2^n listed as follows:

$$f(x_1, x_2, ..., x_n) = [f(0,0,...,0), f(1,0,...,0), f(0,1,...,0), ..., f(1,1,...,1)].$$

$f(x_1, x_2, ..., x_n)$ can also be seen as a multivariate polynomial over F_2, that is

$$f(x_1, x_2, ..., x_n) = a_0 + \sum_{1 \leq i \leq n} a_i x_i + \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j + \cdots + a_{12...n} x_1 x_2 \cdots x_n,$$

where the coefficients $a_0, a_i, a_{ij}, ..., a_{12...n} \in \mathrm{F}_2$. This representation of f is called the algebraic normal form (ANF).

The number of variables in the highest order term with nonzero coefficient is called the algebraic degree of f which is denoted by $\deg(f)$. A Boolean function is affine function if it has the algebraic degree at most 1, and the set of all n-variable affine functions is denoted by A_n.

The support of f is denoted by $\mathrm{supp}(f)=\{x \mid f(x)=1\}$, and the Hamming weight $\mathrm{wt}(f)$ of f is the cardinality of $\mathrm{supp}(f)$.

The Hamming distance between two Boolean functions f and g can be denoted by $\mathrm{d}(f,g) = \mathrm{wt}(f+g)$, where + denotes the addition on F_2 in this paper.

Definition 2.1. [18]For any Boolean function f, Walsh transform can be defined as follows,

$$\mathrm{W}_f(u) = \sum_{x \in \mathrm{F}_2^n} (-1)^{f(x)+x \cdot u} \tag{1}$$

Where the $u \in \mathrm{F}_2^n$, $x \cdot u$ is a inner product x and u.

Definition 2.2.[18]For any Boolean function f, the nonlinearity of f denoted by $\mathrm{NL}(f)$, can be defined as follows,

$$\mathrm{NL}(f)=\min_{g\in A_n} \mathrm{d}(f,g)$$

Equivalently, the nonlinearity of f can also be given by

$$\mathrm{NL}(f)=2^{n-1}-\frac{1}{2}\max_{\omega\in \mathrm{F}_2^n}\left|\mathrm{W}_f(\omega)\right|$$

For two n-variable Boolean functions f and g, g is called an annihilator of f if $f\cdot g=0$ .The set of all annihilators are denoted by $\mathrm{Ann}(f)=\{g\in \mathrm{B}_n \mid f\cdot g=0\}$.

Definition 2.3. [6]The algebraic immunity(AI) of n-variable Boolean function f is denoted by

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

Definition 2.4. Let

$$F_n(x)=\begin{cases}0, & \text{if } \mathrm{wt}(x)\le \dfrac{n}{2};\\ 1, & \text{else.}\end{cases}$$

Then $F_n(x)$ is called the majority function. For an even n, $F_n(x)$ which is an even-variable RSBF with opitimum AI has been defined as follows [9]. Based on some results studied in [8, 9], we have the following proposition.

Proposition 2.5. [8, 9]we have

$$W_{F_n}(u)=\begin{cases}\binom{n}{n/2}, & \text{if } \mathrm{wt}(u)=0;\\ \binom{n}{n/2}, & \text{if } \mathrm{wt}(u)=1;\\ (-1)^{\frac{n}{2}}\binom{n}{n/2}, & \text{if } \mathrm{wt}(u)=n.\end{cases}$$

and for $2\le \mathrm{wt}(u)\le n-1$, we have $\left|W_{F_n}(u)\right|\le \dfrac{1}{n-1}\binom{n}{n/2}$

Definition 2.6. Let $x=(x_1,x_2,...,x_n)\in \mathrm{F}_2^n$, then for any $x_i(1\le i\le n)$ and $0\le k\le n-1$, $\rho_n^k(x_i)$ is defined as

$$\rho_n^k(x_i)=\begin{cases}x_{i+k}, & \text{if } i+k\le n;\\ x_{i+k-n}, & \text{otherwise.}\end{cases}$$

Then we can extend the definition of ρ_n^k on vectors as follows:

$$\rho_n^k(x_1,x_2,...,x_n)=(\rho_n^k(x_1),\rho_n^k(x_2),...,\rho_n^k(x_n))$$

If $\{i_1,i_2,...,i_m\}$ is a subset of $\mathrm{supp}(x)$, then for any $i_j(1\le j\le m)$, $\varphi_n^k(i_j)$ is defined as

$$\varphi_n^k(i_j)=\begin{cases} i_j-k+n, & \text{if } i_j-k\le 0;\\ i_j-k, & \text{otherwise.}\end{cases}$$

then the definition of φ_n^k on set $\{i_1,i_2,...,i_m\}$ can be deduced as

$$\varphi_n^k\{i_1,i_2,...,i_m\}=\{\varphi_n^k(i_1),\varphi_n^k(i_2),...,\varphi_n^k(i_m)\}$$

From the definition of ρ_n^k and φ_n^k, it is obvious that

$$\mathrm{supp}(\rho_n^k(x))=\varphi_n^k(\mathrm{supp}(x))$$

Definition 2.7. For a function $f\in B_n$, if $f(\rho_n^k(x))=f(x)$ holds for all $x\in \mathrm{F}_2^n$ and $1\le k<n$, then f is called rotation symmetric Boolean function(RSBF).

The inputs of a RSBF can be divided into orbits so that each orbit consists of all cyclic shifts of one input. An orbit generated by $x=(x_1,x_2,...,x_n)$ is defined as

$$G_n(x)=\{\rho_n^l(x_1,x_2,...,x_n)\mid 0\le l\le n-1\}$$

3. New construction class of even-variable RSBFs with maximum AI

3.1. Construction

In order to clearly illustrate our constructions of even-variable RSBFs with optimum AI, some notations and lemmas should be given, and from now on , we assume that n is an even positive integer and $n\ge 16$.

Let $H=\left\{h\middle|2\le h\le \lfloor n/4\rfloor-1\right\}$, and the number of elements in H is $M(M=\lfloor n/4\rfloor-3)$.

Define $\lambda_k^{(h)},\nu_k^{(h)}\in \mathrm{F}_2^n$ such that

$$\mathrm{supp}(\lambda_k^{(h)})=\{1,2,...,h\}\cup\{k-h\}\cup\{k,k+1,...,t_k^{(h)}-1\}$$

$$\mathrm{supp}(\nu_k^{(h)})=\{1,2,...,h\}\cup\{k-h\}\cup\{k,k+1,...,t_k^{(h)}-1,t_k^{(h)}\}$$

$k,t_k^{(h)}$ satisfy that

$$\begin{cases} K^h=\left\{k\mid \frac{n}{2}-1<k<\frac{n}{2}+h\right\},\left|K^h\right|=N_1=h\\ t_k^{(h)}=\frac{n}{2}-h+k-2\end{cases}\tag{2}$$

Now we prove the existence of $\lambda_k^{(h)}$ and $\nu_k^{(h)}$:

Proof. According to (2) and the range of h, then $k-h>h+1$ and $n-h-3<t_k^{(h)}<n-2$ which shows $t_k^{(h)}$ exists.

According to the relation $t_k^{(h)}=\frac{n}{2}-h+k-2$, we know

$$\left|\{k,k+1,...,t_k^{(h)}-1,t_k^{(h)}\}\right|=t_k^{(h)}-k+1=\frac{n}{2}-h-1>2$$

So

$$k+1<t_k^{(h)}<n-2.$$

It follows that the definition of $\lambda_k^{(h)}$ and $\nu_k^{(h)}$ exists here and the support of two vectors both contain only one isolated point.

Lemma 3.1. For any $h \in H$ and $k \in K^h$, we have :

1. $|G_n(\lambda_k^{(h)})| = |G_n(\nu_k^{(h)})| = n$.

2.For any $0 \le q \le n-1$. It holds that $\mathrm{supp}(\rho_n^q(\lambda_k^{(h)})) \subseteq \mathrm{supp}(\rho_n^q(\nu_k^{(h)}))$.

Proof . From the definition of $\lambda_k^{(h)}$ and $\nu_k^{(h)}$, it is clearly that the relation 2 is right. The support of two vectors both contain only one isolated point. So the relation 1 is right.

Lemma 3.2. Given $h \in H$, then for any $k \in K^h$ and $0 \le q_1 \ne q_2 \le n-1$, We have

$$\mathrm{supp}(\rho_n^{q_2}(\lambda_k^{(h)})) \not\subset \mathrm{supp}(\rho_n^{q_1}(\nu_k^{(h)}))$$

Proof.

$$\mathrm{supp}(\rho_n^{q_2}(\lambda_k^{(h)})) \not\subset \mathrm{supp}(\rho_n^{q_1}(\nu_k^{(h)}))$$

$$\Leftrightarrow \mathrm{supp}(\rho_n^{q}(\lambda_k^{(h)})) \not\subset \mathrm{supp}(\nu_k^{(h)}), (0 < q \le n-1)$$

$$\Leftrightarrow \varphi_n^{q}(\mathrm{supp}(\lambda_k^{(h)})) \not\subset \mathrm{supp}(\nu_k^{(h)}), (0 < q \le n-1)$$

Suppose that there exists a $q'(0 < q' \le n-1)$ such that $\varphi_n^{q'}(\mathrm{supp}(\lambda_k^{(h)})) \subseteq \mathrm{supp}(\nu_k^{(h)})$.

1)To proof $\varphi_n^{q'}\{k, k+1, ..., t_k^{(h)} - 1\} \subseteq \{k, k+1, ..., t_k^{(h)}\}$.

For the consecutive subset $\varphi_n^{q'}\{k, k+1, ..., t_k^{(h)} - 1\} \subseteq \varphi_n^{q'}(\mathrm{supp}(\lambda_k^{(h)})) \subseteq \mathrm{supp}(\nu_k^{(h)})$ from

$$\begin{cases} |\{k, k+1, ..., t_k^{(h)} - 1\}| = \dfrac{n}{2} - h - 2 > \dfrac{n}{2} - \lfloor n/4 \rfloor - 1, \\ |\{1, 2, ..., h\}| = h < \lfloor n/4 \rfloor - 1. \end{cases}$$

then

$$|\{k, k+1, ..., t_k^{(h)} - 1\}| > |\{1, 2, ..., h\}|.$$

so

$$\varphi_n^{q'}\{k, k+1, ..., t_k^{(h)} - 1\} \subseteq \{k, k+1, ..., t_k^{(h)}\} \quad (3)$$

2)To proof $\varphi_n^{q'}\{1, 2, ..., h\} \subseteq \{k, k+1, ..., t_k^{(h)}\}$.

For another consecutive subset $\varphi_n^{q'}\{1, 2, ..., h\} \subseteq \varphi_n^{q'}(\mathrm{supp}(\lambda_k^{(h)})) \subseteq \mathrm{supp}(\nu_k^{(h)})$ .From

$$q' \ne 0$$

we have

$$\varphi_n^{q'}\{1, 2, ..., h\} \not\subset \{1, 2, ..., h\},$$

then

$$\varphi_n^{q'}\{1,2,...,h\} \subseteq \{k, k+1, ..., t_k^{(h)}\} \tag{4}$$

But for $h \geq 2$, thus

$$|\varphi_n^{q'}\{1,2,...,h\}| + |\varphi_n^{q'}\{k, k+1, ..., t_k^{(h)} - 1\}| > |\{k, k+1, ..., t_k^{(h)}\}|$$

It follows that relations (3) and (4) cannot be satisfied simultaneously. This contradicts with $\varphi_n^{q'}(\mathrm{supp}(\lambda_k^{(h)})) \subseteq \mathrm{supp}(\nu_k^{(h)})$.
Therefore,

$$\varphi_n^{q}(\mathrm{supp}(\lambda_k^{(h)})) \not\subset \mathrm{supp}(\nu_k^{(h)}), (0 < q \leq n-1).$$

Lemma 3.3. Given $h \in H$, then for any $k_1, k_2 \in K^h$ and $k_1 < k_2, 0 \leq q_1, q_2 \leq n-1$, then

$$\mathrm{supp}(\rho_n^{q_2}(\lambda_{k_2}^{(h)})) \not\subset \mathrm{supp}(\rho_n^{q_1}(\nu_{k_1}^{(h)}))$$

Proof.

$$\mathrm{supp}(\rho_n^{q_2}(\lambda_{k_2}^{(h)})) \not\subset \mathrm{supp}(\rho_n^{q_1}(\nu_{k_1}^{(h)}))$$

$$\Leftrightarrow \mathrm{supp}(\rho_n^{q}(\lambda_{k_2}^{(h)})) \not\subset \mathrm{supp}(\nu_{k_1}^{(h)}), (0 \leq q \leq n-1)$$

$$\Leftrightarrow \varphi_n^{q}(\mathrm{supp}(\lambda_{k_2}^{(h)})) \not\subset \mathrm{supp}(\nu_{k_1}^{(h)}), (0 \leq q \leq n-1)$$

Suppose that there exists a $q'(0 \leq q' \leq n-1)$ such that $\varphi_n^{q'}(\mathrm{supp}(\lambda_{k_2}^{(h)})) \subseteq \mathrm{supp}(\nu_{k_1}^{(h)})$
1.If $0 < q' \leq n-1$,

(a)To proof $\varphi_n^{q'}\{1,2,...,h\} \subseteq \{k_1, k_1+1, ..., t_{k_1}^{(h)}\}$.

For the consecutive subset $\varphi_n^{q'}\{1,2,...,h\} \subseteq \varphi_n^{q'}(\mathrm{supp}(\lambda_{k_2}^{(h)})) \subseteq \mathrm{supp}(\nu_{k_1}^{(h)})$,

from

$$\varphi_n^{q'}\{1,2,...,h\} \not\subset \{1,2,...,h\} (0 < q' \leq n-1).$$

then,

$$\varphi_n^{q'}\{1,2,...,h\} \subseteq \{k_1, k_1+1, ..., t_{k_1}^{(h)}\} \tag{5}$$

(b)To proof $\varphi_n^{q'}\{k_2, k_2+1, ..., t_{k_2}^{(h)} - 1\} \subseteq \{k_1, k_1+1, ..., t_{k_1}^{(h)}\}$.

For another consecutive subset $\varphi_n^{q'}\{k_2, k_2+1, ..., t_{k_2}^{(h)} - 1\} \subseteq \varphi_n^{q'}(\mathrm{supp}(\lambda_{k_2}^{(h)})) \subseteq \mathrm{supp}(\nu_{k_1}^{(h)})$, from

$$\begin{cases} |\{k_2, k_2+1, ..., t_{k_2}^{(h)} - 1\}| = \dfrac{n}{2} - h - 2 > \dfrac{n}{2} - \lfloor n/4 \rfloor - 1, \\ |\{1,2,...,h\}| = h < \lfloor n/4 \rfloor - 1. \end{cases}$$

it is clearly that

$$|\{k_2, k_2+1, ..., t_{k_2}^{(h)} - 1\}| > |\{1,2,...,h\}|.$$

so

$$\varphi_n^{q'}\{k_2, k_2+1, ..., t_{k_2}^{(h)}-1\} \subseteq \{k_1, k_1+1, ..., t_{k_1}^{(h)}\}. \quad (6)$$

Since $\varphi_n^{q'}(\mathrm{supp}(\lambda_{k_2}^{(h)}))$ and $\mathrm{supp}(\nu_{k_1}^{(h)})$ also satisfy the conditions listed below,

$$\begin{cases} |\varphi_n^{q'}\{k_2, k_2+1, ..., t_{k_2}^{(h)}-1\}| + |\varphi_n^{q'}\{1,2,...,h\}| = \dfrac{n}{2}-2, \\ |\{k_1, k_1+1, ..., t_{k_1}^{(h)}\}| = \dfrac{n}{2}-h-1, \\ h \geq 2 \end{cases}$$

$$\Rightarrow |\varphi_n^{q'}\{k_2, k_2+1, ..., t_{k_2}^{(h)}-1\}| + |\varphi_n^{q'}\{1,2,...,h\}| > |\{k_1, k_1+1, ..., t_{k_1}^{(h)}\}|.$$

It follows that relations(5)and (6) cannot be satisfied simultaneously. This contradicts with $\varphi_n^{q'}(\mathrm{supp}(\lambda_{k_2}^{(h)})) \subseteq \mathrm{supp}(\nu_{k_1}^{(h)})$

Therefore,

$$\varphi_n^{q'}(\mathrm{supp}(\lambda_{k_2}^{(h)})) \not\subset \mathrm{supp}(\nu_{k_1}^{(h)}), (0 < q' \leq n-1) \quad (7)$$

2.If $q' = 0$

$$\varphi_n^0(\mathrm{supp}(\lambda_{k_2}^{(h)})) = \{1,2,...,h\} \cup \{k_2 - h\} \cup \{k_2, k_2+1, ..., t_{k_2}^{(h)}-1\}$$

$$\mathrm{supp}(\nu_{k_1}^{(h)}) = \{1,2,...,h\} \cup \{k_1 - h\} \cup \{k_1, k_1+1, ..., t_{k_1}^{(h)}\}$$

Since $k_1, k_2 \in \{k \mid \frac{n}{2}-1 < k < \frac{n}{2}+h\}$ and $k_1 < k_2$, so $k_2 - k_1 < h$, thus $k_2 - h < k_1$.

From $k_2 - h \neq k_1 - h$, $k_2 - h > h+1$ and $k_2 - h < k_1$, we have

$$\varphi_n^0(\mathrm{supp}(\lambda_{k_2}^{(h)})) \not\subset \mathrm{supp}(\nu_{k_1}^{(h)}) \quad (8)$$

From relations (7) and (8), therefore,

$$\varphi_n^{q'}(\mathrm{supp}(\lambda_{k_2}^{(h)})) \not\subset \mathrm{supp}(\nu_{k_1}^{(h)}), (0 \leq q' \leq n-1)$$

Now we give our construction class to get $M(M = \lfloor n/4 \rfloor - 3)$ different constructions of even-variable RSBFs with optimum AI which is denoted by $\mathrm{Construction}^{(h)}$.

$\mathrm{Construction}^{(h)}(h \in H)$

Step 1. Let n be an even integer and more than 16.

Step 2. Construct $\lambda_k^{(h)}(k \in K^h)$ such that

$$\mathrm{supp}(\lambda_k^{(h)}) = \{1,2,...,h\} \cup \{k-h\} \cup \{k, k+1, ..., t_k^{(h)}-1\}$$

$$\mathrm{supp}(\nu_k^{(h)}) = \{1,2,...,h\} \cup \{k-h\} \cup \{k, k+1, ..., t_k^{(h)}-1, t_k^{(h)}\}$$

$t_k^{(h)}$ satisfies $t_k^{(h)} - k + h + 2 = \frac{n}{2}$.

Step 3. Let $N_2 = \lfloor n/4 \rfloor$. Construct $l_p \in \mathrm{F}_2^n (1 \le p \le N_2)$ such that

$$\mathrm{supp}(l_p) = \{1, 2, ..., \frac{n}{2} - 1\} \cup \{\frac{n}{2} + p\}.$$

Step 4. Let $B = \{G_n(\lambda_k^{(h)}) \mid k \in K^h\}$ and $C = \{G_n(l_p) \mid 1 \le p \le N_2\}$.
We construct $f(x)$ as follows

$$f(x) = \begin{cases} F_n(x) + 1, & x \in B \cup C, \\ F_n(x), & \text{otherwise.} \end{cases} \tag{9}$$

3.2. The AI of $f(x)$ in Construction$^{(h)}(h \in H)$

Lemma 3.4. [19]Let n be even and let $a_1, ..., a_{\binom{n}{n/2}}$ be an ordering of all vectors of weight $\frac{n}{2}$ in F_2^n, for every $i \in \left(1, 2, ..., \binom{n}{n/2}\right)$, let us define the linear subspace A_i and the flat A_i^o respectively as follows,

$$A_i = \{x \in \mathrm{F}_2^n \mid \mathrm{supp}(x) \subseteq \mathrm{supp}(a_i)\}$$

$$A_i^o = \{x \in \mathrm{F}_2^n \mid \mathrm{supp}(a_i) \subseteq \mathrm{supp}(x)\}$$

Let I, J and K be three disjoint subsets of $\left\{1, 2, ..., \binom{n}{n/2}\right\}$. Assume that, for every $i \in I$, there exists a vector $b_i \ne a_i$ such that $b_i \in A_i \setminus [\bigcup_{i^* < i} A_{i^*}]$. Assume that, for every $j \in J$, there exists a vector $c_j \ne a_j$ such that $c_j \in A_j^o \setminus [\bigcup_{j^* < j} A_{j^*}^o]$. Then the function with support set

$$\{x \in \mathrm{F}_2^n \mid \mathrm{wt}(x) > \frac{n}{2}\} \cup \{a_j \mid j \in J \cup K\} \cup \{b_i \mid i \in I\} \setminus \{c_j \mid j \in J\}$$

has maximum algebraic immunity.

Theorem 3.5. For any $h \in H$, the function $f(x)$ in Construction$^{(h)}(h \in H)$ is an n-variable RSBFs with optimum AI.
Proof. For any $h \in H$.

Let $I = \{1, 2, ..., N_1 \cdot n\}$. For $i \in I$, such that $i = 1 + (k_1 - \frac{n}{2})n + q_1 (k_1 \in K^h, 0 \le q_1 \le n-1)$. we have $b_i = \rho_n^{q_1}(\lambda_{k_1}^{(h)})$ and $a_i = \rho_n^{q_1}(\nu_{k_1}^{(h)})$ Denote by A_i the linear subspace $\{x \in \mathrm{F}_2^n \mid \mathrm{supp}(x) \subseteq \mathrm{supp}(a_i)\}$. Then we have $b_i \ne a_i$ and $b_i \in A_i$. Now we prove $b_i \notin \bigcup_{i^* < i} A_{i^*}$.

Suppose that $\exists i^* < i$ with $b_i \in A_i^*$. Let $i^* = 1 + (k_2 - 1)n + q_2 (k_2 \in K^h, 0 \le q_2 \le n-1)$. Then by the definition of A_{i^*}, we have

$$\mathrm{supp}(\rho_n^{q_1}(\lambda_{k_1}^{(h)})) \subseteq \mathrm{supp}(\rho_n^{q_2}(\nu_{k_2}^{(h)}))$$

Then by lemma 3.2 and 3.3, the above relation implies that $k_1 = k_2, q_1 = q_2$ or $k_1 < k_2$, which contradicts with the fact that $i^* < i$. So we have $b_i \notin \bigcup_{i^* < i} A_{i^*}$.

Let $J=\varnothing$ and $K=\{N_1\cdot n+1, N_1\cdot n+2,...,(N_1+N_2)\cdot n\}$. For $k\in K, k=N_1\cdot n+1+(p_1-1)n+q_1$ $(1\le p_1\le N_2, 0\le q_1\le n-1)$, $a_k=\rho_n^{q_1}(l_{p_1})$.

Then by lemma 3.4 the function with support

$$\{x\in \mathrm{F}_2^n \mid \mathrm{wt}(x)>\frac{n}{2}\}\cup\{a_j \mid j\in J\cup K\}\cup\{b_i \mid i\in I\}\setminus\{c_j \mid j\in J\}$$

has optimum AI, which is equal to say that $f(x)$ has optimum AI.

4. Nonlinearity

Theorem 4.1. Given $h\in H$ .The nonlinearity $\mathrm{NL}(f)$ of the RSBFs in Construction$^{(h)}$ satisfies

$$\mathrm{NL}(f)=2^{n-1}-\binom{n-1}{n/2}+2h$$

Proof. By (1) and (9), we have

$$\begin{aligned} W_f(u)&=\sum_{x\in B\cup C}(-1)^{F_n(x)+1+x\cdot u}+\sum_{x\notin B\cup C}(-1)^{F_n(x)+x\cdot u}\\ &=\sum_{x\in \mathrm{F}_2^n}(-1)^{F_n(x)+x\cdot u}+2\sum_{x\in B\cup C}(-1)^{F_n(x)+1+x\cdot u}\\ &=W_{F_n}(u)-2\sum_{x\in B}(-1)^{x\cdot u}-2\sum_{x\in C}(-1)^{x\cdot u}\end{aligned}$$

Now we compute $W_f(u)$ for different weights of u:

1) $\mathrm{wt}(u)=0$. From Proposition 2.5, it follows that $W_{F_n}(u)=\binom{n}{n/2}$. We have

$$|W_f(u)|=\binom{n}{n/2}-2N_1n-2N_2n$$

2) $\mathrm{wt}(u)=1$. According to Proposition 2.5, it follows that $W_{F_n}(u)=\binom{n}{n/2}$.So

$$\begin{aligned} W_f(u)&=\binom{n}{n/2}-2\sum_{k\in K^h}(n-2\mathrm{wt}(\lambda_k^{(h)}))-2\sum_{1\le p\le N_2}(n-2\mathrm{wt}(l_p))\\ &=\binom{n}{n/2}-2\sum_{k\in K^h}(n-2(\frac{n}{2}-1))\\ &=\binom{n}{n/2}-4N_1.\end{aligned}$$

3) $\mathrm{wt}(u)=n$.By Proposition 2.5, it is clear that $W_{F_n}(u)=(-1)^{\frac{n}{2}}\binom{n}{n/2}$. So

If $\frac{n}{2}$ is odd, then

$$W_f(u)=-\binom{n}{n/2}-2N_1n+2N_2n=-\binom{n}{n/2}+2(N_2-N_1)n$$

If $\frac{n}{2}$ is even, it follows that

$$W_f(u)=\binom{n}{n/2}+2N_1n-2N_2n=\binom{n}{n/2}-2(N_2-N_1)n$$

For any even n and $N_2-N_1\ge 2$ therefore,

$$|W_f(u)| = \binom{n}{n/2} - 2(N_2 - N_1)n < \binom{n}{n/2} - 4N_1$$

4) $2 \le \mathrm{wt}(u) \le n-1$. From Proposition 2.5, we have $W_{F_n}(u) \le \frac{1}{n-1}\binom{n}{n/2}$. Then

$$\begin{aligned} |W_f(u)| &= |W_{F_n}(u) - 2\textstyle\sum_{x\in B}(-1)^{x\cdot u} - 2\sum_{x\in C}(-1)^{x\cdot u}| \\ &\le |W_{F_n}(u)| + 2|\textstyle\sum_{x\in B}(-1)^{x\cdot u}| + 2|\sum_{x\in C}(-1)^{x\cdot u}| \\ &\le \frac{1}{n-1}\binom{n}{n/2} + 2N_1 n + 2N_2 n \\ &< \binom{n}{n/2} - 4N_1 \end{aligned}$$

Comparing the results of four cases. $|W_f(u)|$ is largest when $\mathrm{wt}(u) = 1$. Note that $\binom{n}{n/2} = 2\binom{n-1}{n/2}$, $N_1 = h$ and $\mathrm{NL}(f) = 2^{n-1} - \frac{1}{2}\max_{\omega\in \mathrm{F}_2^n} |W_f(\omega)|$, the nonlinearity $\mathrm{NL}(f)$ satisfies that $\mathrm{NL}(f) = 2^{n-1} - \binom{n-1}{n/2} + 2h$.

5. Conclusion

In this paper, we have presented a new category of even-variable RSBFs with optimum AI in which there are altogether $\lfloor n/4 \rfloor - 3$ different constructions. We have also studied the nonlinearity of our construction. Because there was only one paper [16] that has given a type of even-variable RSBFs with optimum AI in which there are $\frac{n}{2} - 1$ different constructions in all, we hope that our contribution to a new method of construction can be of help to the study of RSBFs.

However, there is still much to be explored in the search for better RSBFs used in the symmetric ciphers. So, how to construct balanced even-variable RSBFs which achieve optimum AI, high nonlinearity, high algebraic degree and resiliency will be our main task in the future.

Acknowledgements

The first author is supported by the Natural Science Foundation of China (No:61103244), the Foundation for Distinguished Young Talents in Higher Education of Guangdong, China (No:LYM11064) and the Academic Innovation Team Construction Project of Shantou University (No:ITC12001).

References

[1] N. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations", Advances in Cryptology-ASIACRYPT 2002, LNCS, vol. 2501, **(2002)**, pp. 267-287.
[2] 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.
[3] W. Mihaljevic and H. Imai, "Cryptanalysis of toyocrypt-HS1 stream cipher", IEICE Trans. Fundam. Electron. Commun., vol. 85-A, no. 1, **(2002)**, pp. 66-73.
[4] N. Courtois, "Cryptanalysis of SFINKS", Information Security and Cryptology—ICISC 2005, LNCS, Springer-Verlag, vol. 3935, **(2006)**, pp. 261-269.
[5] D. K. Dalai, K. C. Gupta and S. Maitra, "Results on algebraic immunity for cryptographically significant Boolean functions", INDOCRYPT 2004, LNCS, vol. 3348, **(2004)**, pp. 92-106.

[6] 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.
[7] 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.
[8] C. Carlet, X. Y. Zeng, C. L. Li and L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity", Designs, Codes and Cryptography, vol. 52, **(2009)**, pp. 303-338.
[9] D. K. Dalai, S. Maitra and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity", Designs, Codes and Cryptography, vol. 40, **(2006)**, pp. 41-58.
[10] L. J. Qu, K. Q. Feng, F. Liu and L. Wang, "Constructing symmetric Boolean functions with maximum algebraic immunity", IEEE Transactions on Information Theory, vol. 55, **(2009)**, pp. 2406-2412.
[11] P. Stanica and S. Maitra, "Rotation symmetric Boolean functions-count and cryptographic properties", Electron.Notes Discrete Math, vol. 15, **(2003)**, pp. 139-145.
[12] S. Sarkar and S. Maitra, "Construction of rotation symmetric Boolean functions with maximun algebraic immunity on odd number of variables", AAECC 2007, LNCS, vol. 4851, Springer, Heidelberg, **(2007)**, pp. 271-280.
[13] S. Sarkar and S. Maitra, "Construction of rotation symmetric Boolean functions with optimal algebraic immunity", Comput. Syst., vol. 12, **(2009)**, pp. 267–284.
[14] Q. Meng, L. S. Chen and F. W. Fu, "Construction of Boolean functions with maximum algebraic immunity", Journal of Software, vol. 21, no. 7, **(2010)**, pp. 1758-1767.
[15] S. Fu, L. Qu, C. Li and B. Sun, "Balanced rotation symmetric Boolean functions with maximum algebraic immunity", IET Inf. Secur., vol. 5, **(2011)**, pp. 93-99.
[16] P. Zhang, D. Dong, S. Fu and C. Li, "New constructions of even-variable rotation symmetric Boolean functions with maximum algebraic immunity", Mathematical and Computer Modelling, vol. 55, **(2012)**, pp. 828-836.
[17] S. Fu, C. Li, K. Matsuura and L. Qu, "Construction of even-variable rotation symmetric Boolean functions with maximum algebraic immunity", Science China Information Sciences, vol. 56, no. 3, **(2013)**, pp. 1-9.
[18] S. Su and X. Tang, "Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity", Des. Codes Cryptogr, http://link.springer.com/article/10.1007\%2Fs10623-012-9727-x.
[19] C. Carlet, "A method of construction of balanced functions with optimum algebraic immunity", Proceedings of the International Workshop on Coding and Cryptography, The Wuyi Mountain, Fujian, China, **(2007)** June 11-15.

Authors

Yindong Chen, 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.

Hongyan Xiang, is a postgraduate student at Shantou University, China. Her research interest is in Cryptology and Information Security.

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