Results on Rotation Symmetric Boolean Functions on Even Number Variable *

Pinhui Ke[1,2] , Zhuling Chang[1,3] Qiaoyan Wen[1]
1.School of Science,Beijing University of Posts and Telecommunications
Beijing, 100876, P. R. China
2.Department of Mathematics,Fujian Normal University
Fuzhou 350007, P. R. China
3.State Key Laboratory of Information Security, Chinese Academy of Sciences
Beijing, 100039, P. R.China
keph@eyou.com , zlchang@eyou.com, wqy@bupt.edu.cn

Abstract

Construction of Boolean functions with cryptographic properties is an important and difficult work. In this paper, we concentrate on rotation symmetric Boolean functions(RSBFs), which are invariant under circular translation of indices. Recent research show that this class of Boolean function is rich in functions of cryptographic significance. In this paper, we consider the RSBFs on even number variable. We show that the matrix ${}_n\mathcal{A}$ may result in a better form after rearrange the representative elements. This allows us to improved the search strategy. At last, some combinatorial results about $\mathcal{P}_n^1$, which only appear in the case n even, are presented in the case $n = 2p$, p be odd prime.

Keywords: Rotation Symmetric Boolean Functions; Correlation Immunity; Walsh Spectra; Algebraic Attack.

1 Introduction

Construction of Boolean functions as a nonlinear filter in design of a cipher is an important and difficult task for cryptography[1] [2].To resist various of attacks, lots of criteria for choosing Boolean functions have been identified,such as balancedness ,algebraic degree, nonlinearity,autocorrelation,correlation immunity,algebraic immunity etc.However there exist trade-offs among these criteria which have received a lot of attentions in Boolean functions literature for a long time(see for example [1]).

Rotation Symmetric Boolean Functions(RSBF) as a new class of functions was introduced in 1998[3],which are invariant under rotation of indices for its input variables.In 1998, Pieprzyk and Qu study RSBFs as components in the round of a hashing algorithm[8].Furthermore,it has been shown that many functions in terms of good cryptographic properties are rich in this class. At Indocrypt 2004[8], it was showed that RSBFs are rich of functions that are strong against algebraic attacks.So many attentions are attracted to these areas.Some important properties of these functions up to 8 variable have been demonstrated in [4].Two important date structure for efficient search strategy of rots bent and CI functions were presented in [5],and they proved the

*Research supported by the National Natural Science Foundation of China(60373059), the National Research Foundation for the Doctoral Program of Higher Education of China(20040013007) and the research foundation of the State Key Laboratory of Information Security..

nonexistence of homogeneous rots bent functions of degree ≥ 3 on a single cycle.Recently,new results on RSBFs for odd number of variables were received in [6].As application of their result,they showed the non existence of (9,3,5,240) RSBF.

As pointed out in [6],the matrix structure presented in their paper cannot be extended for n even and it is an interesting research area.In this paper,we investigate the matrix ${}_n\mathcal{A}$ for n even in detail.We divide g_n representative elements into three classes $\mathcal{P}_n^1, \mathcal{P}_n^2$ and $\mathcal{P}_n^3$,among which $\mathcal{P}_n^1$ is a special class that doesn't appear in the case n odd.We show that after some permutation the matrix ${}_n\mathcal{A}$ result in a better form,denoted as ${}_n\mathcal{A}^\pi$. Although it doesn't have the good structure as the case n odd. It also possess some good properties. This allows us to improved the calculation Walsh spectra of RSBFs.As an example,we compare the computation complexity of search for (6,-,-,-)RSBF by our improved search strategy and by previous search method. At the end of this paper, we present some combinatorial results about the number of elements in P_n^1 in the case $n = 2p$,p be an odd prime.

2 Preliminaries

A Boolean function on n variables may be viewed as a mapping from $V_n = \{0,1\}^n$ into $V_1 = \{0,1\}$. A Boolean function is also interpreted as the output column of its truth table,i.e., a binary string of length 2^n, $f = [f(0,0,\cdots,0), f(1,0,\cdots,0),\cdots, f(1,1,\cdots,1)]$. Also any boolean function $f(x_1,\ldots,x_n)$ can be expressed as one n-variables polynomial

$$f(x_1,\ldots,x_n) = a_0 \oplus \bigoplus_{1\leq i\leq n} a_i x_i \oplus \bigoplus_{1\leq i\neq j\leq n} a_{ij}x_i x_j \oplus \cdots \oplus a_{12\cdots n}x_1x_2\cdots x_n,$$

where the coefficients $a_0, a_{ij},\ldots,a_{12\cdots n} \in F_2$. This representation of $f(x)$ is called the *algebraic normal form*(ANF) of $f(x)$.In the algebraic normal form of $f(x)$, every $x_{i_1}\ldots x_{i_s}$ is called one *monomial*. The *degree* of one monomial is the number of different x_i in it and the degree of one Boolean function $f(x)$ is defined as the maximum degree of monomials in its algebraic normal form.Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function.

The *hamming distance* between two strings,X and Y, is denoted by $d(X,Y) = \#(X \neq Y)$. And the *hamming weight* of a binary string X is the number of ones in X,denoted by $wt(X)$.

The *Walsh transform* of $f(x)$ on $\omega \in F_2^n$ is defined as

$$W_f(\omega) = \sum_{x\in F_2^n} (-1)^{f(x)\oplus\omega\cdot x},$$

in which $\omega\cdot x$ denotes the *inner product* of ω and x.

By the *Walsh transform*,Many properties of Boolean functions can be described.The nonlinearity of f is given by $nl(f) = 2^{n-1} - \frac{1}{2}max_{w\in\{0,1\}^n}|W_f(w)|$. A function is balanced iff $W_f(0) = 0$. A function is m-resilient (respectively m-correlation immune) iff its Walsh spectra satisfies $W_f(w) = 0$,for $0 \leq wt(w) \leq m$(respectively $1 \leq wt(w) \leq m$).

As the notation used in [1][2],we denote an n-variable,m-resilient function with degree d and nonlinearity σ by (n,m,d,σ) function. Further by $[n,m,d,\sigma]$ function,we denote an unbalanced n-variable,m-resilient function with degree d and nonlinearity σ .

2.1 Introduction to Rotation Symmetric Boolean Functions

Let $x_i \in \{0,1\}$ for $1 \leq i \leq n$,we define the permutation $\rho_n^k(x_i)$ as $\rho_n^k(x_i) = x_{i+k}$ mod n. Let$(x_1,x_2,\ldots,x_n) \in \{0,1\}^n$. Then we extend the definition as $\rho_n^k(x_1,x_2,\ldots,x_n) = (\rho_n^k(x_1),\rho_n^k(x_2),$ $\cdots,\rho_n^k(x_n))$.

Definition 2.1 *A Boolean function f is called Rotation Symmetric if for each input $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n, f(\rho_n^k(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n)$ for $1 \le k \le n$.*

let us denote

$$G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n), 1 \le k \le n\}.$$

Note that $G_n(x_1, x_2, \ldots, x_n)$ generate a partition in the input set F_2^n.Each partition consist of all cycle shifts of one element.The number of partitions is denoted by g_n.The lexicographically first element of each partition is considered as the *representative element* $\Lambda_{n,i}$.The *rotation symmetric truth table* is defined as the g_n-bit string $f(\Lambda_{n,0}), f(\Lambda_{n,1}), \cdots, f(\Lambda_{n,g_{n-1}})$. Thus the number of n variable RSBFs is 2^{g_n}.By Burnside lemma,it was shown in [4] that g_n is $\frac{1}{n}\sum_{k|n}\phi(k)2^{\frac{n}{k}}$,where $\phi(k)$ is Eular's *phi*-function.Further denote by $g_{n,w}$ and $h_{n,w}$ the number of partitions of weight w and the number of long cycles of weight w respectively. A recursive calculate formula can be found in [4].Recently a more concrete calculate formula of the number of partitions of size t with element of weight w was presented in [7].

In [4],two matrix ${}_n\mathcal{A}$ and ${}_n\mathcal{B}$ were introduced for efficient calculation of Walsh transform of RSBFs. The matrix ${}_n\mathcal{A}$ was defined as

$${}_n\mathcal{A}_{i,j} = \sum_{x \in G_n(\Lambda_{n,i})} (-1)^{x \cdot \Lambda_{n,i}}.$$

From the definition of RSBFs,we know that the existence of a representative term $x_{i_1}x_{i_2}\cdots x_{i_n}$ implies the existence of all the terms from the set $G_n(x_{i_1}x_{i_2}\cdots x_{i_n})$. So an RSBF can be written as

$$f(x_1, \ldots, x_n) = a_0 + \sum a_1 x_1 \sum a_{1j}x_1x_j + \cdots + a_{12\cdots n}x_1x_2\cdots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\cdots n} \in F_2$.We call it the *short algebraic normal form*(SANF) of an RSBF. The matrix ${}_n\mathcal{B}$ was defined as

$${}_n\mathcal{B}_{i,j} = \bigoplus_{x \in G_n(\Lambda_{n,j})} e|_{\Lambda_{n,i}}.$$

By matrix ${}_n\mathcal{A}$, the Walsh transform for an RSBFs can be calculated from its RSTT as

$$W_f(\Lambda_{n,j}) = \sum_{i=o}^{g_n-1} (-1)_n^{f(\Lambda_{n,i})}\mathcal{A}_{i,j}.$$

In [6] the RSBFs for odd number of variables were considered in detail . Let us permute the rows and columns of ${}_n\mathcal{A}$ in the following ways : the first $\frac{g_n}{2}$ rows and columns correspond to representative elements $\Lambda_{n,i}$ of even weight,and the second $\frac{g_n}{2}$ rows and columns correspond to their complements. Then the new matrix ,denoted as ${}_n\mathcal{A}^\pi$, has a nice structure:

$${}_n\mathcal{A}^\pi = \left(\begin{array}{c|c} {}_n\mathcal{H} & {}_n\mathcal{H} \\ \hline {}_n\mathcal{H} & -{}_n\mathcal{H} \end{array}\right).$$

Let us divide the RSTT of an RSBF into two parts σ_1 and σ_2,such that RSTT=$\sigma_1 \parallel \sigma_2 \in \{0,1\}^{g_n}$,and $\sigma_1, \sigma_2 \in \{0,1\}^{\frac{g_n}{2}}$. Defined binary string σ_i^* as follows:

$$\sigma_{i_j}^* = \left\{\begin{array}{ll} 1, & \sigma_{i_j} = 0 \\ -1, & \sigma_{i_j} = 1 \end{array}\right., i = 1, 2, 1 \le j \le \frac{g_n}{2}.$$

We refer $w_1 = \sigma_1^*\ {}_n\mathcal{H}$ and $w_2 = \sigma_2^*\ {}_n\mathcal{H}$ as *partial Walsh transform*(${}_pWT$). Then the Walsh transform for any input w can be calculated as :

$$W_f(w) = ((w_1 + w_2) \parallel (w_1 - w_2)).$$

In this way , the number of operations can be reduced to $2 \cdot (\frac{g_n}{2})^2 + g_n \le g_n^2$.Furthermore the structure of ${}_n\mathcal{A}^\pi$ allowed us to look insight into the Walsh transform of an RSBF.

3 Walsh transform of RSBFs

3.1 Matrix ${}_n\mathcal{A}$ for n even

As mentioned in last paragraph, the investigation of ${}_n\mathcal{A}$ for n odd is very useful. However it cannot extended to the case n even[6]. Boolean functions with even number variable are of lot interest as evident from [1, 2].Naturally, we want to know weather there exist RSBF with the same parameter. In order to make our search strategy more efficient, we also need to investigate the matrix ${}_n\mathcal{A}$ for n even.Before we present our conclusion, let us see a simple example when n be 6. The collections of representative elements and matrix ${}_n\mathcal{A}$ are list following:

i	0	1	2	3	4	5	6
$\Lambda_{6,i}$	000000	000001	000011	000101	000111	001001	001011
i	7	8	9	10	11	12	13
$\Lambda_{6,i}$	001101	001111	010101	010111	011011	011111	111111

Tabular 1: collection of representative elements

$${}_6\mathcal{A}=\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
6 & 4 & 2 & 2 & 0 & 2 & 0 & 0 & -2 & 0 & -2 & -2 & -4 & -6\\
6 & 2 & 2 & -2 & 2 & -2 & -2 & -2 & 2 & -6 & -2 & -2 & 2 & 6\\
6 & 2 & -2 & 2 & -2 & -2 & -2 & -2 & -2 & 6 & 2 & -2 & 2 & 6\\
6 & 0 & 2 & -2 & 0 & -6 & 0 & 0 & -2 & 0 & 2 & 6 & 0 & -6\\
3 & 1 & -1 & -1 & -3 & 3 & 1 & 1 & -1 & -3 & -1 & 3 & 1 & 3\\
6 & 0 & -2 & -2 & 0 & 2 & -4 & 4 & 2 & 0 & 2 & -2 & 0 & -6\\
6 & 0 & -2 & -2 & 0 & 2 & 4 & -4 & 2 & 0 & 2 & -2 & 0 & -6\\
6 & -2 & 2 & -2 & -2 & -2 & 2 & 2 & 2 & 6 & -2 & -2 & -2 & 6\\
2 & 0 & -2 & 2 & 0 & -2 & 0 & 0 & 2 & 0 & -2 & 2 & 0 & -2\\
6 & -2 & -2 & 2 & 2 & -2 & 2 & 2 & -2 & -6 & 2 & -2 & -2 & 6\\
3 & -1 & -1 & -1 & 3 & 3 & -1 & -1 & -1 & 3 & -1 & 3 & -1 & 3\\
6 & -4 & 2 & 2 & 0 & 2 & 0 & 0 & -2 & 0 & -2 & -2 & 4 & -6\\
1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1
\end{bmatrix}$$

Tabular 2: matrix of ${}_6\mathcal{A}$

Let us rearrange representative elements as follows:

i	0	1	2	3	4	5	6
$\Lambda_{6,i}$	000000	000011	000101	001001	111111	001111	010111
i	7	8	9	10	11	12	13
$\Lambda_{6,i}$	110110	000001	001011	011111	001101	000111	010101

Tabular 3: rearrangement of representative elements

According to this order of representative elements , we get the ${}_6\mathcal{A}^{\pi}$:

$$
{}_6\mathcal{A}^{\pi}= \left[\begin{array}{cccc|cccc|cccc|cc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
6 & 2 & -2 & -2 & 6 & 2 & -2 & -2 & 2 & -2 & 2 & -2 & 2 & -6 \\
6 & -2 & 2 & -2 & 6 & -2 & 2 & -2 & 2 & -2 & 2 & -2 & -2 & 6 \\
3 & -1 & -1 & 3 & 3 & -1 & -1 & 3 & 2 & -2 & 2 & -2 & -3 & -3 \\
\hline
6 & 2 & 2 & 2 & 6 & 2 & 2 & 2 & 4 & 0 & -4 & 0 & 0 & 0 \\
6 & -2 & -2 & 2 & 6 & -2 & -2 & 2 & 0 & -4 & 4 & 0 & 0 & 0 \\
\hline
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\
6 & 2 & -2 & -2 & 6 & 2 & -2 & -2 & -2 & 2 & -2 & 2 & -2 & 6 \\
6 & -2 & 2 & -2 & 6 & -2 & 2 & -2 & -2 & 2 & -2 & 2 & 2 & -6 \\
3 & -1 & -1 & 3 & 3 & -1 & -1 & 3 & -2 & 2 & -2 & 2 & 3 & 3 \\
\hline
6 & 2 & 2 & 2 & 6 & 2 & 2 & 2 & -4 & 0 & 4 & 0 & 0 & 0 \\
6 & -2 & -2 & 2 & 6 & -2 & -2 & 2 & 0 & 4 & -4 & 0 & 0 & 0 \\
\hline
6 & 2 & -2 & -6 & 6 & 2 & -2 & -6 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & -2 & 2 & -2 & 2 & -2 & 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right]
$$

Tabular 4: matrix of ${}_6\mathcal{A}^{\pi}$

It is clear that matrix ${}_6\mathcal{A}^{\pi}$ has a better structure than ${}_6\mathcal{A}$. In order to derive the general conclusion , Let us define following notation:

$\mathcal{P}_n = \{\Lambda_{n,i} | 1 \le i \le g_n\}$,

$\mathcal{P}_n^1 = \{\Lambda_{n,i} | G_n(\Lambda_{n,i}) = G_n(\overline{\Lambda}_{n,i}), 1 \le i \le g_n\}$,

$\mathcal{P}_n^{11} = \{\Lambda_{n,i} | G_n(\Lambda_{n,i}) = G_n(\overline{\Lambda}_{n,i}), wt(\Lambda_{n,i})\ is\ even, 1 \le i \le g_n\}$,

$\mathcal{P}_n^{12} = \{\Lambda_{n,i} | G_n(\Lambda_{n,i}) = G_n(\overline{\Lambda}_{n,i}), wt(\Lambda_{n,i})\ is\ odd, 1 \le i \le g_n\}$,

$\mathcal{P}_n^2 = \{\Lambda_{n,i} | G_n(\Lambda_{n,i}) \in \mathcal{P}_n \backslash \mathcal{P}_n^1, wt(\Lambda_{n,i})\ is\ even, 1 \le i \le g_n\}$,

$\mathcal{P}_n^3 = \{\Lambda_{n,i} | G_n(\Lambda_{n,i}) \in \mathcal{P}_n \backslash \mathcal{P}_n^1, wt(\Lambda_{n,i})\ is\ odd, 1 \le i \le g_n\}$, where $\overline{x}$ denote the complement of x. For simplicity , we write $11\cdots1$ as 1 . So $\overline{X} = 1 \bigoplus X$. By above notation, $\mathcal{P}_n = \cup_{i=1}^3 \mathcal{P}_n^i$. Following Lemma will be useful.

Lemma 3.1 *Let $x \in F_2^n$ and $G_n(\Lambda_{n,i})$ be the partition generated by $\Lambda_{n,i}$, then we have*

$$\sum_{x \in G_n(\overline{\Lambda}_{n,i})} (-1)^{\alpha \cdot x} = (-1)^{wt(\alpha)} \sum_{x \in G_n(\Lambda_{n,i})} (-1)^{\alpha \cdot x}$$

$$\sum_{x \in G_n(\Lambda_{n,i})} (-1)^{\overline{\alpha} \cdot x} = (-1)^{wt(\Lambda_{n,i})} \sum_{x \in G_n(\Lambda_{n,i})} (-1)^{\alpha \cdot x}$$

Proof: Noted that each element in $G_n(\Lambda_{n,i})$ has the same weight. The proof is easy to verified.

Theorem 3.1 *For n even, the matrix ${}_n\mathcal{A}^{\pi}$ is of the form*

$$\left[\begin{array}{cccc} A & A & C & C \\ A & A & -C & -C \\ B & -B & D & -D \\ B & -B & D & D \\ E & E & 0 & 0 \\ F & -F & 0 & 0 \end{array}\right] \begin{array}{cc} & \\ & \\ G & H \\ & \\ & \\ & \end{array}$$

where A, B, C, D, E, F, G, H are some arrays.

Proof: For elements in $\mathcal{P}_n^2(\mathcal{P}_n^3$ respectively),their complement elements are also in $\mathcal{P}_n^2(\mathcal{P}_n^3$ respectively).So $\mathcal{P}_n^2$(or $\mathcal{P}_n^3$) are consist of some element and their complement elements. Let us rearrange representative element as

$$x_{i_1} \cdots x_{i_{\frac{|\mathcal{P}_n^2|}{2}}} \overline{x}_{i_1} \cdots \overline{x}_{i_{\frac{|\mathcal{P}_n^2|}{2}}} x_{j_1} \cdots x_{j_{\frac{|\mathcal{P}_n^3|}{2}}} \overline{x}_{j_1} \cdots \overline{x}_{j_{\frac{|\mathcal{P}_n^3|}{2}}} x_{k_1} \cdots x_{k_{|\mathcal{P}_n^{11}|}} x_{l_1} \cdots x_{l_{|\mathcal{P}_n^{12}|}}.$$

1. If $\Lambda_{n,i} \in \mathcal{P}_n \backslash \mathcal{P}_n^1$, there are following four cases:
   (a) If $\Lambda_{n,i} \in \mathcal{P}_n^2$ and $wt(\alpha)$ be even, then ${}_n\mathcal{A}^\pi_{\overline{\Lambda}_{n,i},\alpha} =_n \mathcal{A}^\pi_{\Lambda_{n,i},\alpha}$,${}_n\mathcal{A}^\pi_{\Lambda_{n,i},\overline{\alpha}} =_n \mathcal{A}^\pi_{\Lambda_{n,i},\alpha}$by Lemma 3.1.
   (b) If $\Lambda_{n,i} \in \mathcal{P}_n^2$ and $wt(\alpha)$ be odd, then ${}_n\mathcal{A}^\pi_{\overline{\Lambda}_{n,i},\alpha} = -{}_n\mathcal{A}^\pi_{\Lambda_{n,i},\alpha}$,${}_n\mathcal{A}^\pi_{\Lambda_{n,i},\overline{\alpha}} =_n \mathcal{A}^\pi_{\Lambda_{n,i},\alpha}$by Lemma 3.1.
   (c) If $\Lambda_{n,i} \in \mathcal{P}_n^3$ and $wt(\alpha)$ be even, then ${}_n\mathcal{A}^\pi_{\overline{\Lambda}_{n,i},\alpha} =_n \mathcal{A}^\pi_{\Lambda_{n,i},\alpha}$, ${}_n\mathcal{A}^\pi_{\Lambda_{n,i},\overline{\alpha}} = -{}_n\mathcal{A}^\pi_{\Lambda_{n,i},\alpha}$by Lemma 3.1.
   (d) If $\Lambda_{n,i} \in \mathcal{P}_n^3$ and $wt(\alpha)$ be odd, then ${}_n\mathcal{A}^\pi_{\overline{\Lambda}_{n,i},\alpha} = -{}_n\mathcal{A}^\pi_{\Lambda_{n,i},\alpha}$,${}_n\mathcal{A}^\pi_{\Lambda_{n,i},\overline{\alpha}} =_n \mathcal{A}^\pi_{\Lambda_{n,i},\alpha}$by Lemma 3.1.
2. If $\Lambda_{n,i} \in \mathcal{P}_n^1$, $G_n(\Lambda_{n,i})$ is consist of two part, say I and its complement $\overline{I}$.There are following two cases :
   (a) If $wt(\alpha)$ be even, then ${}_n\mathcal{A}^\pi_{\Lambda_{n,i},\overline{\alpha}} =_n \mathcal{A}^\pi_{\Lambda_{n,i},\alpha}$by Lemma 3.1.
   (b) If $wt(\alpha)$ be odd, then${}_n\mathcal{A}^\pi_{\Lambda_{n,i},\alpha} = \sum_{x\in I}(-1)^{\alpha\cdot x} + \sum_{x\in\overline{I}}(-1)^{\alpha\cdot x} = \sum_{x\in I}(-1)^{\alpha\cdot x} + (-1)^{wt(\alpha)}\sum_{x\in I}(-1)^{\alpha\cdot x} = 0$.

Thus the proof is completed.

Corollary 3.1 *For even n ,the number of $1-$CI RSBFs is at least $2^{g_n-(\frac{|\mathcal{P}_n^2|+|\mathcal{P}_n^3|}{2})}$.*

Proof:Each binary string of length n which weight is 1 belongs to partition $G_n(1,0,\cdots,0)$. By theorem 1, the claim is easily proved.

Corollary 3.2 *[6] For odd n,the matrix ${}_n\mathcal{A}^\pi$ is of the form ${}_n\mathcal{A}^\pi = \left(\begin{array}{c|c} {}_n\mathcal{H} & {}_n\mathcal{H} \\ \hline {}_n\mathcal{H} & -{}_n\mathcal{H} \end{array}\right)$.*

Proof: For odd n, $wt(\overline{X}) \neq wt(X)$. So $\mathcal{P}_n^1$ is empty. Furthermore, if $\Lambda_{n,i} \in \mathcal{P}_n^2$, $\overline{\Lambda}_{n,i} \in \mathcal{P}_n^3$. Similar to the proof of theorem 1, the corollary follows.

For large n, the cost to form the matrix ${}_n\mathcal{A}$ cannot be ignore. By theorem 1, we are able to get matrix ${}_n\mathcal{A}^\pi$ with less time and space complexity. On the other hand, it can be used to reduce the computation complexity when we calculate the Walsh transform of RSBFs.

3.2 Improved search strategy for cryptographic important RSBFs

As we point out in section 2, many cryptographic properties can be presented by Walsh spectra. So if we are able to compute the Walsh spectra efficiently, we have an efficient search strategy for cryptographic important Boolean functions.

A search strategy for cryptographic important RSBFs is given in [5]:

1. choose a candidate RSBF(say f) represented by its SANF.
2. use ${}_n\mathcal{B}$ to get the RSTT of f from SANF.
3. use ${}_n\mathcal{A}$ and the RSTT of f to analysis the Walsh spectra of f.

By Matrix ${}_n\mathcal{A}^\pi$ instead of ${}_n\mathcal{A}$, we are able to reduce the number of operations when we calculate the Walsh spectra of an RSBF. So we modify the last step in following way:

$3^{'}$. use ${}_n\mathcal{A}^\pi$ and the RSTT of f to analysis the Walsh spectra of f.

In the case of 6-variable, we need 196 operation to get the Walsh spectra of a fixed RSBFs by matrix ${}_6\mathcal{A}$. By matrix ${}_6\mathcal{A}^\pi$, the operation number may be reduced to nearly 112.

More concretely, for element in $\mathcal{P}_n^2 \cup \mathcal{P}_n^3$, the operation needed to calculate the Walsh spectra may be reduced to half by ${}_n\mathcal{A}^\pi$. For element in $\mathcal{P}_n^1$, it needed to be taken additional consider.

4 Combinatorial results about $\mathcal{P}_n^1$

In this section, we derive some combinatorial results about the $\mathcal{P}_n^1$ in the special case $n = 2p$, where p is an odd prime.

Lemma 4.1 *Let $n = 2p$, p be odd prime . If $u \in \mathcal{P}_n^1$, then u must be the form $a\overline{a}$, where a is a binary string of length p.*

Proof: Let m be the least integer such that $\rho_n^m u = u$. Then m equals to 2,p or $2p$. For $u \in \mathcal{P}_n^1$, there exist an integer t such that $1 \bigoplus u = \rho_n^t u$. Thus $\rho_n^{n-2t} u = u$. We need to consider following three cases:

1. If $m = 2$, then $u = 0101 \cdots 01$ and each odd t satisfy the condition.
2. If $m = p$, by the minimum of m,we have p divide $n - 2t$. Therefore $t = p$ or $2p$. If $t = 2p$, we have $u = 1 \bigoplus u$. That is impossible. If $t = p$, by the assumption $m = p$, we also derive the contradiction $u = 1 \bigoplus u$. So both the cases are impossible.
3. If $m = 2p$, similar to the case 2, $t = p$ or $2p$. If $t = 2p$, we derive the contradiction $u = 1 \bigoplus u$. If $t = p$, it is clear that u must be the form $a\overline{a}$.

Thus the lemma is proved.

Theorem 4.1 *Let $n = 2p$, p be odd prime. Then $|\mathcal{P}_n^1| = \frac{2^{p-1}-1}{p} + 1$.*

Proof: By Lemma 4.1, we know that each element in $\mathcal{P}_n^1$ must be the form $a\overline{a}$. Denote $M = \{a\overline{a} \mid a \text{ be binary string of length } p\}$. Let the group $G_n = \{\rho_n^t, 1 \le t \le p-1\}$ act on M. It is sufficient to proof that the number of the orbits is $|\mathcal{P}_n^1| = \frac{2^{p-1}-1}{p} + 1$. Let $C(\rho_n^t)$ denote the number of elements in M which are invariant under permutation $\rho_n^t, 1 \le t \le n$. If $gcd(n,t) = 1$ or p, $C(\rho_n^t)$ equals 0. If $gcd(n,t) = 2$, $C(\rho_n^t) = 2$. There are $p-1$ such t, i.e.,$t = 2i, 1 \le t \le p-1$. If $gcd(n,t) = n$, $C(\rho_n^t) = |M| = 2^p$. By Burnside Lemma, $|\mathcal{P}_n^1| = \frac{2^{p-1}-1}{p} + 1$.

5 Conclusion

In this paper, we studied the RSBFs on even number variable. The matrix ${}_n\mathcal{A}$ plays an important role in the search strategy of cryptographic important RSBFs. We proved that the matrix ${}_n\mathcal{A}$ may result in a better form after rearrange the representative elements. Our results can be used to reduce the computation complexity when calculate the Walsh spectra of a RSBF. And we present some combinatorial results about $\mathcal{P}_n^1$, which doesn't appear in the case n odd. Further study on the $\mathcal{P}_n^1$ for general n will be interesting.

References

[1] P.Sarkar and S.Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology-EUROCRYPT 2000*,volume 1807 of Lecture Notes in Computer Science,pages 485-506.Springer-Verlag,2000.

[2] P.Sarkar and S.Maitra. Nonlinear bounds and construction of resilient Boolean functions. In *Advances in Cryptology-CRYPTO 2000*,volume 1880 of Lecture Notes in Computer Science,pages 515-532.Springer-Verlag,2000.

[3] E.Filiol and C.Fontaine. Highly nonlinear balanced Boolean function with a good correlation immunity.In *Advances in Cryptology-EUROCRYPT 1998*, Lecture Notes in Computer Science,1998.

[4] P.Stănică and S.Maitra. Rotation Symmetric Boolean Functions-Count and Cryptographic properties. In *R.C.Bose centenary Symposium on Discrete Mathematics and Applications*,December 2002. Electronic Notes in Discrete Mathematics, Elsevier,Volume 15.

[5] P.Stănică , S.Maitra and J.Clark. Results on rotation symmectric bent and correlation immune boolean functions.In*Fast software Encryption 2004*, volume 3017 of Lecture Notes in computer Science, pages 161-177. Springer-Verlag,2004.

[6] A.Maximov,M.Hell and S.Maitra. Plateaued rotation symmetric boolean functions on odd number of variables. Avaiable at IACR eprint server,eprint.iacr.org,no.2004/144,25 June 2004,2004.

[7] A.Maximov. Classes of plateaued rotation symmetric boolean functions under transformation of walsh spectra , avaiable at http://eprint.iacr.org/2004/354.

[8] Josef Pieprzyk and Cheng xin Qu. Rotation-symmetric functions and fast hashing. In *proceedings of the Third Australatian Conference on Information Security and Privacy*,pages 169-180, Springer-Verlag, 1998.

[9] K.G.Gupta,D.K.Dalai and S.Maitra. Results on algebraic immunity for cryptographically significant boolean functions.*Indocrypt-2004*.