SCIENCE CHINA
Information Sciences

• RESEARCH PAPERS •

March 2010 Vol. 53 No. 3: 537–545
doi: 10.1007/s11432-010-0045-5

On the number of rotation symmetric Boolean functions

FU ShaoJing[1*], LI Chao[1,2] & QU LongJiang[1,3]

[1]*Science College of National University of Defense Technology, Changsha* 410073*, China;*
[2]*State Key Laboratory of Information Security, Beijing* 100039*, China;*
[3]*National Mobile Communications Research Laboratory, Southeast University, Nanjing* 210096*, China*

Received July 7, 2009; accepted October 28, 2009; published online March 1, 2010

Abstract Rotation symmetric Boolean functions (RSBFs) have been used as components of different cryptosystems. This class of functions are invariant under circular translation of indices. In this paper, we investigated balanced RSBFs and 1st order correlation immune RSBFs. Based on constructive techniques, we give an accurate enumeration formula for n-variable balanced RSBFs when n is a power of a prime. Furthermore, an original and efficient method to enumerate all n-variable (n prime) 1st order correlation-immune functions is presented. The exact number of 1st order correlation immune RSBFs with 11 variables is 69250471565504788252252503741297645110776847738055208 00 and the number of 13 variables has 189 digits. Then for more variables, we also provide a significant lower bound on the number of 1st order correlation immune RSBFs.

Keywords cryptography, rotation symmetry, correlation immunity, balancedness

Citation Fu S J, Li C, Qu L J. On the number of rotation symmetric Boolean functions. Sci China Inf Sci, 2010, 53: 537–545, doi: 10.1007/s11432-010-0045-5

1 Introduction

A variety of criteria for choosing Boolean functions with cryptographic applications (for secret key cryptosystems) have been identified. These are balancedness, nonlinearity, autocorrelation, correlation immunity, algebraic degree, etc. The trade-offs among these criteria have received a lot of attention in Boolean function literature for a long time [1–3]. The more the criteria to be taken into account, the more difficult the problem is to obtain a Boolean function satisfying these properties.

It has been found recently that the class of rotation symmetric Boolean functions (RSBFs) is extremely rich in terms of cryptographically significant Boolean functions. These functions have been analyzed in [4]. The nonlinearity of these Boolean functions was studied and some encouraging results were achieved. The study in [4] has been extended in [5–9] and some important properties of RSBFs have been demonstrated. On the other hand, Pieprzyk and Qu [10] studied RSBFs as components in the rounds of a hashing algorithm and research in this direction was later continued in [11].

In the case with every cryptographic property, we are interested in counting the objects satisfying that property. This motivates us to look at Boolean functions satisfying some criteria and try to select

*Corresponding author (email: shaojing1984@yahoo.cn)

functions necessary for a cryptographic design. We need to know how big the pool of choices is and how to generate functions in that pool.

It is clear that there are 2^{2^n} Boolean functions on n-variable and under no circumstances (with current compute power) is it possible to search them exhaustively for $n \geqslant 7$ to check some desired properties. However, the number of RSBFs is about $2^{\frac{2^n}{n}}$ and it is possible to search the space with a much better efficiency.

In [5], Stanica and Maitra gave many counting results of RSBFs; they obtained the number of homogeneous RSBFs with given algebraic degree, and showed that it is easy to get a 7-variable, 2-resilient RSBFs with nonlinearity 56, which were formerly considered as a function not easy to search for. Since the space for 9-variable in the rotation symmetric class is too large for us to execute exhaustive search, Stanica et al. exploited an simulated annealing technique in [7]. For the first time some interesting results were obtained for 9-variable correlation immune functions. We here work in the direction at enumeration of RSBFs and provide better results than those of existing work. Our results reduce a lot the search space of RSBFs with 1st order properties and we can obtain the counting results up to 13-variable.

The remainder of this paper is organized as follows. Section 2 provides basic definitions and notations. In section 3, we study the balanced RSBFs and get the enumeration formulas when the number of input variables is a power of a prime, and we also get the lower bounds on the number of balanced RSBFs. In section 4, we study the 1st order correlation immune RSBFs, and provide the exact number of 1st order correlation immune RSBFs with 11 variables and 13 variables. Then for more variables, we also provide a lower bounds on the number of 1st order correlation immune RSBFs. Section 5 concludes this paper.

2 Preliminaries

Let $\mathbb{F}_2$ be the binary finite field. The vector space of dimension n over $\mathbb{F}_2$ is denoted by $\mathbb{F}_2^n$. A Boolean function on n variables may be viewed as a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. A Boolean function $f(x_1, x_2, \ldots, x_n)$ is also interpreted as the output column of its truth table, that is, a binary string of length 2^n having the form:

$$\{f(0,\ldots,0),\quad f(0,\ldots,1),\ \ldots,\ f(1,\ldots,1)\}.$$

The weight of f is the number of ones in its output column, and is denoted by $wt(f)$.

Definition 1. An n-variable Boolean function f is balanced if and only if $wt(f) = 2^{n-1}$.

Let us denote the addition operator over $\mathbb{F}_2$ by $+$. An n-variable Boolean function $f(x_1, \ldots, x_n)$ can be seen as a multivariate polynomial over $\mathbb{F}_2$, that is,

$$f(x_1,\ldots,x_n) = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1\leqslant i<j\leqslant n} a_{i,j} x_i x_j + \cdots + a_{1,2,\cdots,n} x_1 x_2 \cdots x_n,$$

where the coefficients a_0, a_i, ..., $a_{i,j}$, ..., $a_{1,2,\cdots,n}$ are constant in $\mathbb{F}_2$. This representation of f is called the algebraic normal form (ANF) of f.

Let $x = (x_1, \ldots, x_n)$ and $w = (w_1, \ldots, w_n)$ both belong to $\mathbb{F}_2^n$ and $x \cdot w = x_1 w_1 + x_2 w_2 + \cdots + x_n w_n$. The Walsh transform of an n-variable function f is a real valued function defined as

$$W_f(w) = \sum_{x\in F_2^n} (-1)^{f(x)+x\cdot w}.$$

Definition 2. A function $f(x_1, \ldots, x_n) \in B_n$ is mth order correlation immune (CI) if and only if its Walsh transform satisfies

$$W_f(w) = 0, \quad \text{for } 1 \leqslant wt(w) \leqslant m.$$

If $x_i \in F_2$ for any $1 \leqslant i \leqslant n$, and $0 \leqslant k \leqslant n-1$, we define

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

Let $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. Then we can extend the definition of ρ_n^k on tuples and monomials as follows:

$$\rho_n^k(x_1, \ldots, x_n) = (\rho_n^k(x_1), \ldots, \rho_n^k(x_n)),$$

and

$$\rho_n^k(x_{i_1} x_{i_2} \cdots) = \rho_n^k(x_{i_1})\rho_n^k(x_{i_2}) \cdots .$$

Definition 3. A Boolean function $f(x_1, \ldots, x_n)$ is called rotation symmetry if for each input $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and any $0 \leqslant k \leqslant n-1$, $f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n)$.

Note that there are 2^n different input values corresponding to a function. Let us define $G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 0 \leqslant k \leqslant n-1\}$, that is, the orbit of $(x_1, x_2, \ldots, x_n)$ under the action of ρ_n^k, $0 \leqslant k \leqslant n-1$. It is clear that $G_n(x_1, x_2, \ldots, x_n)$ generates a partition in the set $\mathbb{F}_2^n$. Let g_n be the number of such partitions. According to Burnside lemma, the number of n-variable RSBFs is

$$2^{g_n}, \text{ where } g_n = \frac{1}{n} \sum_{t|n} \phi(t) 2^{\frac{n}{t}},$$

where $\phi(.)$ is Euler's phi-function. It is obvious that $\#G_n(x_1, x_2, \ldots, x_n) \leqslant n$, and we call $G_n(x_1, x_2, \ldots, x_n)$ an m-cycle if $\#G_n(x_1, x_2, \ldots, x_n) = m$. For example, $G_4(1,0,0,0)$, $G_4(1,1,0,0)$, $G_4(1,0,1,1)$ are 4-cycles, whereas, $G_4(0,0,0,0)$, $G_4(1,1,1,1)$ are 1-cycles.

3 Enumeration of balanced RSBFs

In this section, we will study the balanced RSBFs. We start with some basic technical discussion. Let h_d be the number of d-cycles. Obviously d is a proper divisor of n and $\sum_{d|n} h_d = g_n$. The following theorem has been shown in [5].

Theorem 1 [5]**.** If $n = p^r$, then $h_1 = 2$, $h_{p^i} = \frac{2^{p^i} - 2^{p^{i-1}}}{p^i} (1 \leqslant i \leqslant r-1)$, $h_{p^r} = p^{-r}(2^{p^r} + \sum_{j=1}^{r} \phi(p^j) 2^{p^{r-j}}) - \sum_{j=1}^{r-1} h_{p^i} - 2$.

To get balanced RSBFs, we need to partition g_n into 2 groups such that each group consists of 2^{n-1} vectors. Ref. [7] presented the following results of the number of balanced RSBFs.

Lemma 1 [7]**.** Let N_n be the number of n-variable balanced RSBFs. Then

(1) $n = p$, p is an odd prime.

$$N_n = 2 \begin{pmatrix} (2^p - 2)/p \\ (2^{p-1} - 2)/p \end{pmatrix}.$$

(2) $n = p^r (r > 1)$, p is an odd prime. Then

$$N_n \geqslant 2 \prod_{i=1}^{r} \begin{pmatrix} h_{p^i} \\ h_{p^i}/2 \end{pmatrix},$$

where $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

Lemma 1 does not give accurate enumeration formulas; it just gets a lower bound. Now we will give an accurate enumeration formula for $n = p^r (r > 1, p \text{ prime})$.

Let Θ be the equation system as follow:

$$\Theta : \begin{cases} \sum_{i=0}^{r} z_i p^i = 2^{p^r - 1}, \\ z_i \in \mathbb{Z}, 0 \leqslant z_i \leqslant h_{p^i}, \quad 0 \leqslant i \leqslant r. \end{cases}$$

Let $\{(z_0^{(1)}, z_1^{(1)}, \ldots, z_r^{(1)}), (z_0^{(2)}, z_1^{(2)}, \ldots, z_r^{(2)}), \ldots, (z_0^{(T)}, z_1^{(T)}, \ldots, z_r^{(T)})\}$ be the set of the solutions of Θ. Then we have the following result on the number of n-variable balanced RSBFs.

Theorem 2. Let $n = p^r$ (p prime) and N_n be the number of n-variable balanced RSBFs. Then

$$N_n = \sum_{j=1}^{T} \prod_{i=0}^{r} \begin{pmatrix} h_{p^i} \\ z_i^{(j)} \end{pmatrix}.$$

Proof. To find N_n, basically, we try to divide 2^n vectors into two groups A_n and B_n such that $\#A_n = \#B_n = 2^{n-1}$. Of course, the vectors in the same cycle must be in the same group since the function is a RSBF.

Let $\Lambda_i (0 \leqslant i \leqslant r)$ be the set of p^i-cycles. It follows from Theorem 1 that $\#\Lambda_0 = 2$, $\#\Lambda_i = \frac{2^{p^i} - 2^{p^{i-1}}}{p^i} (1 \leqslant i \leqslant r-1)$, $\#\Lambda_r = p^{-r}(2^{p^r} + \sum_{j=1}^{r} \phi(p^j) 2^{p^{r-j}}) - \sum_{j=1}^{r-1} h_{p^j} - 2$. For a fixed solution $(z_0^{(j)}, z_1^{(j)}, \ldots, z_r^{(j)})$, we can construct A_n, B_n as follows:

(A_n) Select $z_0^{(j)}$ 1-cycles from Λ_0, $z_1^{(j)}$ p-cycles from Λ_1, …, $z_r^{(j)}$ p^r-cycles from Λ_r, and regard the vectors in these cycles as the elements of A_n.

(B_n) There are $h_1 - z_0^{(j)}$ 1-cycles in the rest of Λ_0, $h_p - z_1^{(j)}$ p-cycles in the rest of Λ_1, …, $h_{p^r} - z_r^{(j)}$ p^r-cycles in the rest of Λ_r. Regard the vectors in these cycles as the elements of B_n.

Now we define n-variable function $f(x)$ as

$$f(x) : \{x | f(x) = 0\} = A_n, \{x | f(x) = 1\} = B_n.$$

Then $f(x)$ is a balanced RSBF since $\#A_n = \#B_n = 2^{n-1}$, and the number of balanced RSBFs constructed by A_n and B_n equals the ways to choose A_n, B_n, that is,

$$\prod_{i=0}^{r} \binom{h_{p^i}}{z_i^{(j)}}.$$

Given two solutions $(z_0^{(k_1)}, z_1^{(k_1)}, \ldots, z_r^{(k_1)}) \neq (z_0^{(k_2)}, z_1^{(k_2)}, \ldots, z_r^{(k_2)})$, without loss of generality, let $z_r^{(k_1)} \neq z_r^{(k_2)}$. The corresponding A_n is different, so the corresponding two balanced RSBFs are different. Hence, the total number of RSBFs constructed by the construction above is

$$N_n = \sum_{j=1}^{T} \prod_{i=0}^{r} \begin{pmatrix} h_{p^i} \\ z_i^{(j)} \end{pmatrix}.$$

Now we show that any n-variable($n = p^r, r > 1$) balanced RSBFs can be obtained via the construction of A_n and B_n. Given a balanced RSBF $f(x)$, let $A_n = \{x | f(x) = 0\}$, and denote A_n^* by

$$A_n^* = \{G_n(x_1, \ldots, x_n) | (x_1, \ldots, x_n) \in A_n\}.$$

Let $z_i = \#\{A_n^* \bigcap \Lambda_i\}$. Then it is easy to show that $(z_0, \ldots, z_r)$ is a solution of the equation system Θ.

Hence, we finish the proof.

When r becomes larger, solving the equation system Θ will take a lot of CPU time. In this case, we give a lower bound on the number of RSBFs by finding some special solutions of Θ instead of completely solving the equation systems. And our lower bound is better than the lower bound in [7].

Theorem 3. Let $n = p^r$ ($r > 1$),

(1) If p is an odd prime, then

$$N_n \geqslant 4 \sum_{j=2}^{r-1} \left(\sum_{l=1}^{\lfloor \frac{h_{p^j}}{2p} \rfloor} \begin{pmatrix} h_{p^j} \\ h_{p^j}/2 - lp \end{pmatrix} \begin{pmatrix} h_{p^{j+1}} \\ h_{p^{j+1}}/2 + l \end{pmatrix} \prod_{\substack{1 \leqslant i \leqslant r \\ i \neq j \pm 1}} \binom{h_{p^i}}{h_{p^i}/2} \right) + 2 \prod_{1 \leqslant i \leqslant r} \begin{pmatrix} h_{p^i} \\ h_{p^i}/2 \end{pmatrix}.$$

(2) If $p = 2$, then

$$N_n \geqslant 4 \sum_{j=3}^{r-1} \left(\sum_{l=1}^{\lfloor \frac{h_{2^j}}{4} \rfloor} \begin{pmatrix} h_{2^j} \\ h_{2^j}/2 - 2l \end{pmatrix} \begin{pmatrix} h_{2^{j+1}} \\ h_{2^{j+1}}/2 + l \end{pmatrix} \prod_{\substack{3 \leqslant i \leqslant r \\ i \neq j \pm 1}} \binom{h_{2^i}}{h_{2^i}/2} \right) + 2 \prod_{3 \leqslant i \leqslant r} \begin{pmatrix} h_{2^i} \\ h_{2^i}/2 \end{pmatrix}.$$

Proof. (1) When p is an odd prime, $2 \mid h_1 = 2$, and $2 \mid h_{p^i} = 2^{p^i} - 2^{p^{i-1}} \Rightarrow 2 \mid h_{p^i} = \frac{2^{p^i} - 2^{p^{i-1}}}{p^i} (1 \leqslant i \leqslant r-1)$. It is obvious that $2 \mid g_{p^r} = \frac{1}{p^r} \sum_{t \mid p^r} \phi(t) 2^{\frac{p^r}{t}}$. Thus,

$$2 \mid \left(g_{p^r} - \sum_{i=0}^{r-1} h_{p^i} \right) \Rightarrow 2 \mid h_{p^r}.$$

Note that $(1, \frac{h_p}{2}, \ldots, \frac{h_{p^r}}{2})$ is a solution of Θ since $\sum_{i=0}^{r} h_{p^i} p^i = 2^{p^r}$. And if $\lfloor \frac{h_{p^i}}{2p} \rfloor \geqslant 1$, for each integer $1 \leqslant l \leqslant \lfloor \frac{h_{p^i}}{2p} \rfloor$,

$$\left(1, h_p, \ldots, \frac{h_{p^i}}{2} - lp, \frac{h_{p^{i+1}}}{2} + l, \ldots, \frac{h_{p^r}}{2}\right),$$

and

$$\left(1, h_p, \ldots, \frac{h_{p^i}}{2} + lp, \frac{h_{p^{i+1}}}{2} - l, \ldots, \frac{h_{p^r}}{2}\right)$$

are also solutions of Θ, then according to Theorem 2, we get the lower bound on the number of balanced RSBFs as follows:

$$N_n \geqslant 2 \sum_{j=2}^{r-1} \left(\sum_{l=1}^{\lfloor \frac{h_{p^j}}{2p} \rfloor} \binom{h_{p^j}}{h_{p^j}/2 - lp} \binom{h_{p^{j+1}}}{h_{p^{j+1}}/2 + l} \prod_{\substack{1 \leqslant i \leqslant r \\ i \neq j \pm 1}} \binom{h_{p^i}}{h_{p^i}/2} \right)$$

$$+ 2 \sum_{j=2}^{r-1} \left(\sum_{l=1}^{\lfloor \frac{h_{p^j}}{2p} \rfloor} \binom{h_{p^j}}{h_{p^j}/2 + lp} \binom{h_{p^{j+1}}}{h_{p^{j+1}}/2 - l} \prod_{\substack{1 \leqslant i \leqslant r \\ i \neq j \pm 1}} \binom{h_{p^i}}{h_{p^i}/2} \right) + 2 \prod_{1 \leqslant i \leqslant r} \binom{h_{p^i}}{h_{p^i}/2}.$$

Note that

$$\binom{h_{p^j}}{h_{p^j}/2 + lp} = \binom{h_{p^j}}{h_{p^j}/2 - lp,}, \quad \binom{h_{p^{j+1}}}{h_{p^{j+1}}/2 - l} = \binom{h_{p^{j+1}}}{h_{p^{j+1}}/2 + l}.$$

We can simplify the above results and finish the first part proof of the theorem.

(2) If $p = 2$, then $2 \mid h_1 = 2$, $2 \nmid h_2 = 1$, $2 \nmid h_{2^2} = 3$, and it is clear that

$$2 \mid h_{2^i} = \frac{2^{2^i} - 2^{2^{i-1}}}{2^i} (3 \leqslant i \leqslant r-1).$$

Then we can show that

$$2 \mid g_{2^r} = 2^{-r} \left(\sum_{i=1}^{r} (2^i - 2^{i-1}) 2^{2^{r-i}} + 2^{2^r} \right).$$

Thus,

$$2 \left| \left(g_{2^r} - \sum_{i=0}^{r-1} h_{2^i} \right) \Rightarrow 2 \right| h_{2^r}.$$

Now it can be shown that $(2, 1, 1, \frac{h_{2^3}}{2}, \ldots, \frac{h_{2^r}}{2})$ is a solution of Θ. The remaining part of proof is similar to the case where p is an odd prime.

4 Enumeration of 1st order correlation immune RSBFs

Note that there are g_n cycles, and consider the lexicographical first element of each cycles as the representative element. We denote these representative elements by π_i where i varies from 0 to $g_n - 1$ and representative elements are again arranged lexicographically. That is, in the example of section 2, $\pi_0 = (0,0,0,0)$, $\pi_1 = (1,0,0,0)$, $\pi_2 = (1,1,0,0)$, $\pi_3 = (1,0,1,0)$, $\pi_4 = (1,1,1,0)$, $\pi_5 = (1,1,1,1)$. We

define $\Delta_n(w)$ as the set of cycles with representative elements having weight w and denote $\#\Delta_n(w)$ by $g_n(w)$. It can be found in [5] that $g_n(w) = \frac{1}{n}\binom{n}{w}$ if $\gcd(n, w) = 1$, $1 \leqslant w \leqslant n$ and $g_n(0) = g_n(n) = 1$. To get the 1st order correlation immune RSBFs, we first need the following lemma.

Lemma 2 [7]. An n-variable rotation symmetric Boolean function f is 1st order correlation immune if and only if $\sum_{i=0}^{g_n-1}(-1)^{f(\pi_i)}\frac{n-2wt(\pi_i)}{m_i} = 0$, where $m_i = \frac{n}{\#G_n(\pi_i)}$.

Theorem 4. Let n be an odd prime and $F_n = k_0 + \sum_{w=1}^{\frac{n-1}{2}}(n-2w)k_w$, where k_i is the number of 0 value at output corresponding to $\Delta_n(i)$. Then number of 1st order correlation immune RSBFs NC_n satisfies

$$NC_n = \sum_{0\leqslant t\leqslant T}\Big(\sum_{F_n=t}\prod_{w=0}^{\frac{n-1}{2}}\binom{g_n(w)}{k_w}\Big)^2,$$

where $T = g_n(0) + \sum_{w=1}^{\frac{n-1}{2}}(n-2w)g_n(w)$.

Proof. When n is an odd prime, we know that $g_n = \frac{2^n-2}{n} + 2$, and there are $\frac{2^n-2}{n}$ n-cycles and two 1-cycles (all zero, and all one). In order to get the 1st order correlation immune RSBFs, we should assign 0 or 1 value at output such that $\sum_{i=0}^{g_n-1}(-1)^{f(\pi_i)}\frac{n-2wt(\pi_i)}{m_i} = 0$, where $m_i = \frac{n}{\#G_n(\pi_i)}$. Since n is an odd prime, we have $\#G_n(\pi_i) = n$ for $1 \leqslant i \leqslant g_n - 1$, and $\#G_n(\pi_0) = \#G_n(\pi_n) = 1$. Thus,

$$\frac{n-2wt(\pi_i)}{m_i} = n - 2wt(\pi_i)(1 \leqslant i \leqslant g_n - 1),$$
$$\frac{n-2wt(\pi_0)}{m_0} = 1, \frac{n-2wt(\pi_{g_n-1})}{m_{g_n-1}} = -1.$$

Note that $n - 2wt(\pi_i) = n - 2wt(\pi_j)$ if $G_n(\pi_i)$ and $G_n(\pi_j)$ are in the same $\Delta_n(w)$. So the number of 1st order correlation immune RSBFs depends on the assignment of 0 value at output corresponding to $\Delta_n(i)$. Note the assignment of 0 value at output: $\Delta_n(0) : k_0$, …, $\Delta_n(\frac{p-1}{2}) : k_{\frac{p-1}{2}}$, $\Delta_n(\frac{p+1}{2}) : k_{\frac{p+1}{2}}$, …, $\Delta_n(n) : k_n$.

Then we have

$$\sum_{i=0}^{g_n-1}(-1)^{f(\pi_i)}\frac{n-2wt(\pi_i)}{m_i} = 0 \Rightarrow \sum_{w=0}^{n}\sum_{\pi_i\in\Delta_n(w)}(-1)^{f(\pi_i)}\frac{n-2wt(\pi_i)}{m_i} = 0$$
$$\Rightarrow k_0 + \sum_{w=1}^{n-1}(n-2w)k_w - k_n = 0.$$

It is clear that $n - 2w > 0$ if $w \leqslant \frac{n-1}{2}$. So we get

$$k_0 + \sum_{w=1}^{\frac{n-1}{2}}(n-2w)k_w = \sum_{w=\frac{n+1}{2}}^{n-1}(2w-n)k_w + k_n.$$

Denote $H_n = k_n + \sum_{w=\frac{n+1}{2}}^{n-1}(2w-n)k_w$. Then we have the number of 1st order correlation immune RSBFs as follows:

$$\sum_{0\leqslant k_0\leqslant g_n(0)}\cdots\sum_{0\leqslant k_n\leqslant g_n(n)}\sum_{F_n=H_n}\prod_{w=0}^{n}\binom{g_n(w)}{k_w}.$$

Let $T = \max\{F_n(k_0, \ldots, k_{\frac{n-1}{2}}) | 0 \leqslant k_0 \leqslant g_n(0), \ldots, 0 \leqslant k_n \leqslant g_n(n)\}$. It is obvious that $T = F_n(g_n(0), \ldots, g_n(\frac{n-1}{2}))$. Then,

$$\sum_{0\leqslant k_0\leqslant g_n(0)}\cdots\sum_{0\leqslant k_n\leqslant g_n(n)}\sum_{F_n=H_n}\prod_{w=0}^{n}\binom{g_n(w)}{k_w} = \sum_{0\leqslant t\leqslant T}\sum_{F_n=t}\prod_{w=0}^{\frac{n-1}{2}}\binom{g_n(w)}{k_w}\sum_{H_n=t}\prod_{w=\frac{n+1}{2}}^{n}\binom{g_n(w)}{k_w}$$

$$= \sum_{0\leqslant t\leqslant T}\Big(\sum_{F_n=t}\prod_{w=0}^{\frac{n-1}{2}}\binom{g_n(w)}{k_w}\Big)^2.$$

As we know, there are 2^{g_n} RSBFs for n-variable RSBFs. Thus, when $n \geqslant 9$, the complete space of RSBFs is too large to search. However, with the enumeration results in Theorem 4, we can obtain some interesting count results by running program in a space of size $\prod_{w=1}^{\frac{n-1}{2}}(g_n(w)+1)$ instead of searching the whole space of RSBFs.

Let us now consider 7-variable RSBFs. Note that $g_7(0)=1$, $g_7(1)=1$, $g_7(2)=3$, $g_7(3)=5$. Thus we need to investigate a space of size $\prod_{w=0}^{3}(g_7(w)+1)=96$.

Next we consider 11-variable RSBFs. Note that $g_{11}(0)=1$, $g_{11}(1)=1$, $g_{11}(2)=5$, $g_{11}(3)=15$, $g_{11}(4)=30$, $g_{11}(5)=42$. Thus we need to investigate a space of size $\prod_{w=0}^{5}(g_{11}(w)+1)=511872$.

For 13-variable RSBFs, we have $g_{13}(0)=1$, $g_{13}(1)=1$, $g_{13}(2)=6$, $g_{13}(3)=22$, $g_{13}(4)=55$, $g_{13}(5)=99$, $g_{13}(6)=132$. Then we need to investigate a space of size $\prod_{w=0}^{6}(g_{13}(w)+1)=479651200$, which takes almost one hour to complete the search on a single Pentium 1.8 GHz computer with 512 MB RAM using window-xp operating system.

For 17-variable RSBFs, we need to investigate a space of size $\prod_{w=0}^{8}(g_{17}(w)+1)=90734193508880700$. This space is extremely large with respect to our current implementation.

Table 1 presents the number of 1st order correlation immune RSBFs for $n=11$ and $n=13$. To the best of our knowledge this is the first time this value is reported. However, when $n \geqslant 17$, we cannot obtain the exact number, so we try to give an estimation of the number.

Theorem 5. Let n be an odd prime. Then number of 1st order correlation immune RSBFs NC_n satisfies

$$\begin{aligned}NC_n \geqslant \sum_{w^*=2}^{\frac{n-3}{2}}\sum_{i=\pm1}\Bigg[&\prod_{\substack{0\leqslant w\leqslant (n-1)/2,\\ w\neq w^*, w\neq w^*\pm1}}\sum_{k=0}^{g_n(w)}\binom{g_n(w)}{k}^2\\ &\times\sum_{k=0}^{g_n(w^*-1)}\binom{g_n(w^*-1)}{k}\binom{g_n(w^*-1)}{k+i}\times\sum_{k=0}^{g_n(w^*)}\binom{g_n(w^*)}{k}\binom{g_n(w^*)}{k-2i}\\ &\times\sum_{k=0}^{g_n(w^*+1)}\binom{g_n(w^*+1)}{k}\binom{g_n(w^*+1)}{k+i}\Bigg]+\prod_{w=0}^{\frac{n-1}{2}}\sum_{k=0}^{g_n(w)}\binom{g_n(w)}{k}^2.\end{aligned}$$

Proof. Note that $\frac{n-2wt(\pi_i)}{k_i}=-\frac{n-2wt(\pi_j)}{k_j}$ if $G_n(\pi_i)\in\Delta_n(w)$ and $G_n(\pi_j)\in\Delta_n(n-w)$. If we have the same number of 0 value at output corresponding to $\Delta_n(w)$ and $\Delta_n(n-w)$, then $\sum_{i=0}^{g_n-1}(-1)^{f(\pi_i)}\frac{n-2wt(\pi_i)}{k_i}=0$, and therefore we have the following assignment to get 1st order correlation immune RSBFs: $\Delta_n(0):k_0$, $\Delta_n(1):k_1$, …, $\Delta_n(\frac{p-1}{2}):k_{\frac{p-1}{2}}$, $\Delta_n(\frac{p+1}{2}):k_{\frac{p-1}{2}}$, …, $\Delta_n(n-1):k_1$, $\Delta_n(0):k_0$.

Table 1 The number of 1st order CI RSBFs

n	Number
7	75150
11	692504715655047882522525037 4
	1297645110776847738055208 00
13	157163506345076984621659016834 22
	380013520912864377452385732971 11
	826486151636726033523999659077678
	795057158269092333962225274878 84
	646738476995680823970336495542 67
	247339090727216854765583678 06
17	Unable to obtain

For the assignment above we can show that the number of possible options for a pair $\Delta_n(w)$ and $\Delta_n(n-w)$ is $\sum_{k=0}^{g_n(w)}\binom{g_n(w)}{k}^2$, and then we can construct $\prod_{w=0}^{\frac{n-1}{2}}\sum_{k=0}^{g_n(w)}\binom{g_n(w)}{k}^2$ 1st order correlation immune RSBFs.

If $G_n(\pi_i)\in\Delta_n(w+1)$, $G_n(\pi_j)\in\Delta_n(w)$ and $G_n(\pi_k)\in\Delta_n(w+1)$, then it follows that $wt(\pi_i)+wt(\pi_k)=2wt(\pi_j)$, so

$$(n-2wt(\pi_i))+(n-2wt(\pi_k))=2(n-2wt(\pi_j)).$$

Now we can have two other assignments of output to be 1st order correlation immune RSBFs,

1. $\Delta_n(0):k_0$, $\Delta_n(1):k_1$, …, $\Delta_n(\frac{p-1}{2}):k_{\frac{p-1}{2}}$, $\Delta_n(\frac{p+1}{2}):k_{\frac{p-1}{2}}$,…,$\Delta_n(w^*-1):k_{w^*-1}+1$, $\Delta_n(w^*):k_{w^*}-2$, $\Delta_n(w^*+1):k_{w^*+1}+1$, …, $\Delta_n(n-1):k_1$, $\Delta_n(n):k_0$.

2. $\Delta_n(0):k_0$, $\Delta_n(1):k_1$, …, $\Delta_n(\frac{p-1}{2}):k_{\frac{p-1}{2}}$, $\Delta_n(\frac{p+1}{2}):k_{\frac{p+1}{2}}$,…, $\Delta_n(w^*-1):k_{w^*-1}-1$, $\Delta_n(w^*):k_{w^*}+2$, $\Delta_n(w^*+1):k_{w^*+1}-1$, …, $\Delta_n(n-1):k_1$, $\Delta_n(n):k_0$.

For the former assignment, we can construct

$$\sum_{w^*=2}^{\frac{n-3}{2}}\prod_{\substack{0\leqslant w\leqslant(n-1)/2,\\ w\neq w^*,w\neq w^*\pm1}}\sum_{k=0}^{g_n(w)}\binom{g_n(w)}{k}^2\sum_{k=0}^{g_n(w^*)}\binom{g_n(w^*)}{k}\binom{g_n(w^*)}{k+2}\times\sum_{k=0}^{g_n(w^*+1)}\binom{g_n(w^*+1)}{k}\binom{g_n(w^*+1)}{k-1}\sum_{k=0}^{g_n(w^*-1)}\binom{g_n(w^*-1)}{k}\binom{g_n(w^*-1)}{k-1}$$

1st order correlation immune RSBFs. For the latter assignment, we can construct

$$\sum_{w^*=2}^{\frac{n-3}{2}}\prod_{\substack{0\leqslant w\leqslant(n-1)/2,\\ w\neq w^*,w\neq w^*\pm1}}\sum_{k=0}^{g_n(w)}\binom{g_n(w)}{k}^2\sum_{k=0}^{g_n(w^*-1)}\binom{g_n(w^*-1)}{k}\binom{g_n(w^*-1)}{k+1}\times\sum_{k=0}^{g_n(w^*)}\binom{g_n(w^*)}{k}\binom{g_n(w^*)}{k-2}\sum_{k=0}^{g_n(w^*+1)}\binom{g_n(w^*+1)}{k}\binom{g_n(w^*+1)}{k+1}$$

1st order correlation immune RSBFs.

Thus, we get the count.

At last, we compare the counting results obtained by [7], Theorem 4, and Theorem 5 in Table 2.

5 Conclusions

In this paper, we have obtained some counting results on the rotation symmetric Boolean functions. For the counting of balanced RSBFs, we get an accurate enumeration formula for n-variable balanced RSBFs when n is a power of a prime, and we also obtained a lower bounds on the number of balanced RSBFs. For n-variables (n prime), we provide the exact number of 1st order correlation immune RSBFs with 11 variables and 13 variables and provide the lower bounds of the 1st order correlation immune RSBFs for more variables. But for general n(n is not prime), the lengths of the cycles in $\Delta_n(w)$ are not same; thus, exploiting a similar strategy for 1st order correlation immune RSBFs will be invalid. On the other hand, how to count the balanced RSBFs for general n should be another interesting problem for the future research.

Table 2 The number of 1st order CI RSBFs

n	Paper [7]	Theorem 5	Theorem 4
7	$\geqslant$20160	$\geqslant$26460	=75150
11	$\geqslant 3.1\cdot10^{52}$	$\geqslant 1.3\cdot10^{53}$	$\approx 6.9\cdot10^{54}$
13	$\geqslant 2.5\cdot10^{184}$	$\geqslant 1.7\cdot10^{185}$	$\approx 1.6\cdot10^{188}$
17	$\geqslant 1.1\cdot10^{2311}$	$\geqslant 1.2\cdot10^{2312}$	–
19	$\geqslant 6.5\cdot10^{8293}$	$\geqslant 8.5\cdot10^{8294}$	–

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 60803156), the Open Research Fund of State Key Laboratory of Information Security (Grant No. 01–07), and the Open Research Fund of National Mobile Communications Research Laboratory of Southeast University (Grant No. W200807).

References

1 Clark J, Jacob J, Stepney S, et al. Evolving Boolean functions satisfying multiple criteria. In: INDOCRYPT 2002, LNCS, vol. 2551. Berlin: Springer-Verlag, 2002. 246–259
2 Clark J, Jacob J, Maitra S, et al. Almost Boolean functions: The design of Boolean functions by spectral inversion. In: the 2003 Congress on Evolutionary Computation (CEC 2003), Vol. 3. Newport Beach, California, USA, 2003. 2173–2180
3 Maitra S, Pasalic E. Further constructions of resilient Boolean functions with very high nonlinearity. IEEE Trans Inf Theory, 2002, 48: 1825–1834
4 Filiol E, Fontaine C. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In: Advances in Cryptology-EUROCRYPT 98, LNCS, Vol. 1403. Berlin: Springer-Verlag, 1998. 475–488
5 Stanica P, Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties. Discrete Math Appl, 2008, 156: 1567–1580
6 Stanica P, Maitra S. A constructive count of rotation symmetric functions. Inf Process Lett, 2003, 88: 299–304
7 Stanica P, Maitra S, Clark J. Results on rotation symmetric bent and correlation immune Boolean functions. In: Fast Software Encryption Workshop (FSE 2004), LNCS, Vol. 3017. Berlin: Springer-Verlag, 2004. 161–177
8 Maximov A, Hell M, Maitra S. Plateaued rotation symmetric Boolean functions on odd number of variables. In: First Workshop on Boolean Functions: Cryptography and Applications, BFCA 05, Rouen, France, 2005. 83–104
9 Dalai D K, Maitra S, Sarkar S. Results on rotation symmetric bent functions. In: Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06, Rouen, France, 2006. 137–156
10 Pieprzyk J, Qu C X. Fast hashing and rotation-symmetric runctions. J Univ Comput Sci, 1999, 5: 20–31
11 Cusick T W, Stanica P. Fast evaluation, weights and nonlinearity of rotation-symmetric functions. Discrete Math, 2002, 258: 289–301