Chapter 6

Generalized Rotation Symmetric Boolean Functions

6.1 Introduction

In 2007, Kavut et al.[75] generalized the concept of rotation symmetry and defined a class of Boolean functions namely k-rotation symmetric Boolean functions, where k is a positive integer dividing n. They found several 9-variable Boolean functions having nonlinearity of 242 [76] in this class. Further applications of the k-rotation symmetric functions to coding theory and S-box design were given in [77]. Recently Cusick and Bryan Johns studied the 2-MRS Boolean functions [78]. They studied the cubic 2-MRS functions in $2n$ variables generated by a monomial $x_1x_rx_s$ with $1 < r < s$ and r and s not both odd. They gave a complete description of affine equivalence for these functions and proved that the sequence of Hamming weights of these functions satisfies a linear recursion with integer coefficients.

In this chapter, we study the class of k-rotation symmetric Boolean functions and obtain the exact number of homogeneous k-rotation symmetric Boolean functions using Polya's enumeration theorem. We analyze the weight and nonlinearity of 2-rotation symmetric Boolean functions, in particular quadratic 2-MRS Boolean functions and give a complete characterization of the weight and nonlinearity for

these functions. We observed that the weight of 2-MRS Boolean functions of degree d where $d \geqslant 3$ is same as their nonlinearity.

6.2 k-Rotation Symmetric Boolean functions

Definition 6.1. *(Cyclic rotation)* Let $x_i \in F_2$, for any $0 \leq i \leq n-1$ and $1 \leq k \leq n$ we define

$$\rho_n^k(x_i) = \begin{cases} x_{i+k} & \text{if } i+k \leq n-1 \\ x_{i+k-n} & \text{if } i+k \geq n \end{cases}$$

Definition 6.2. *(k-rotation symmetric Boolean function)*
Let $1 \leq k \leq n$, be a positive integer dividing n. An n-variable Boolean function f is called k-rotation symmetric(k-RotS) if f is invariant under ρ_n^k i.e, for each input $(x_0, x_1, ..., x_{n-1}) \in F_2^n$,

$$f(\rho_n^k(x_0, x_1, ..., x_{n-1})) = f(x_0, x_1, ..., x_{n-1})$$

Note that k-rotation symmetric Boolean function f possess the same value corresponding to each of the subsets generated from the k-rotational symmetry. The inputs of a k-rotation symmetric Boolean function can be divided into orbits so that each orbit consists of all k-cyclic shifts of one input. An orbit generated by $(x_0, x_1, ..., x_{n-1})$ is $G_n(x_0, x_1, ..., x_{n-1}) = \left\{\rho_n^{tk}(x_0, x_1, ..., x_{n-1})/0 \leq t \leq \frac{n}{k} - 1\right\}$ and the function possesses the same value for all inputs in the same orbit. Let $g_n^{(k)}$ be the number of such orbits. Then the number of k- rotation symmetric Boolean functions is $2^{g_n^{(k)}} - 1$. Kavut [75] has evaluated the value of $g_n^{(k)}$ as $g_n^{(k)} = \frac{k}{n} \sum_{d|\frac{n}{k}} \phi(d) 2^{\frac{n}{d}}$. We prove that the value of $g_n^{(k)}$ can also be derived using Polya's enumeration theorem by evaluating the cycle index polynomial of the cyclic group of order $\frac{n}{k}$ generated by ρ_n^k at $x = 2$.

6.3 Enumeration of k-Rotation Symmetric Boolean Functions

Note that if the ANF of the k-RotS function contains a term $x_{i_1}x_{i_2}...x_{i_d}$ then it has all the terms from the orbit $\left\{\rho_n^{tk}(x_{i_1}x_{i_2}...x_{i_d})/0 \leq t \leq \frac{n}{k}-1\right\}$ of $x_{i_1}x_{i_2}...x_{i_d}$. The greatest degree of all terms of f in ANF is called the algebraic degree of f. A function is said to be homogeneous if all monomials in the ANF of the function are of same degree. First consider $G_n(x_0, x_1, ..., x_{n-1})$, where $wt(x_0, x_1, ..., x_{n-1})$ is exactly w. Note that in this way we get a partition over the n- bit binary strings of weight w. Let us consider that the number of such partitions is $g_{n,w}^k$. This means that the degree w monomials can be divided into $g_{n,w}^k$ different classes.The value of $g_{n,w}^k$ can be efficiently calculated using Polya's enumeration theorem .

Theorem 6.3. *The number of orbits $G_n(x_0, x_1, ..., x_{n-1})$, such that $wt(x_0, x_1, ..., x_{n-1}) = w$ under the action of the cyclic group of order $\frac{n}{k}$ generated by ρ_n^k over $\mathbb{F}_2^n$ is given by*

$$g_{n,w}^k = \frac{k}{n}\sum_{d|r}\phi(d)\begin{pmatrix} \frac{n}{d} \\ \frac{w}{d} \end{pmatrix}$$

where $r = gcd(\frac{n}{k}, w)$

Proof. Let X be the set of all monomials in n-variables and G be the cyclic group of permutations on n- elements generated by ρ_n^k. Then the cycle index polynomial of G is given by

$$Z_G(t_1, t_2, ..., t_n) = \frac{k}{n}\sum_{d|\frac{n}{k}}\phi(d)t_d^{\frac{n}{d}}$$

Consider the finite field $\mathbb{F}_2$ as the set of colors. Let us define the weight for each colors as $w(0) = 0$ and $w(1) = y$.Then by Polya's theorem, pattern index of nonequivalent colorings of X under G is given by

$$I = Z_G\left(1+y, 1+y^2, ..., 1+y^n\right) = \frac{k}{n}\sum_{d|\frac{n}{k}}\phi(d)\left(1+y^d\right)^{n/d}.$$

Then the number of orbits of weight w is exactly the coefficient of y^w in the expansion of I. By noting the points that when $d = 1$ the term y^w occurs exactly once in the expansion of I with the coefficient $\begin{pmatrix} n \\ w \end{pmatrix}$ and when $d > 1$ the expansion of I contributes a term y^w if and only if $r = gcd(\frac{n}{k}, w)$ is greater than one. Hence by summing over all divisors of r we can deduce the sum of coefficients of y^w in the expansion of I as

$g_{n,w} = \frac{k}{n} \sum_{d|r} \phi(d) \begin{pmatrix} \frac{n}{d} \\ \frac{w}{d} \end{pmatrix}$ where $r = gcd(\frac{n}{k}, w)$ □

Corollary 6.4. *The number of n-variable homogeneous k-rotation symmetric Boolean functions of degree $w \geq 1$ is $2^{g^k_{n,w}} - 1$.*

6.4 Weight and Nonlinearity of Quadratic 2-MRS Functions

A Boolean function on n-variables is said to be 2-rotation symmetric if it is invariant under the action of ρ^2. A Boolean function is said to be 2-monomial rotation symmetric (2-MRS) if it is generated by applying the powers of ρ^2 to a single monomial. Note that n should be an even integer. Let f be the quadratic 2-MRS Boolean function generated by $x_a x_b$ then the weight and nonlinearity of f depends only on the difference $b - a$ and n.

Theorem 6.5. *Let f be an n-variable quadratic 2-MRS Boolean function generated by the monomial $x_a x_b$ where $b-a$ is odd. Then f has weight same as its nonlinearity and is given by*

$$wt(f) = nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$$

Proof. Let $b - a = 2k + 1$. Then the Boolean function f is given by

$$f(x_0, x_1, ..., x_{n-1}) = x_a x_{a+2k+1} + x_{a+2} x_{a+2k+3} + ... + x_{a+n-2} x_{a+2k+n-1}$$

If we rename the variables as $x_a = y_0, x_{a+2} = y_2, ..., x_{a+n-2} = y_{n-2}$, $x_{a+2k+1} = y_1, x_{a+2k+3} = y_3, ..., x_{a+2k+n-1} = y_{n-1}$, then f is equivalent to $f \equiv y_0y_1 + y_2y_3 + ... + y_{n-2}y_{n-1}$. So by lemma 5 of [61] f is bent and its weight is same as its nonlinearity. Thus

$$wt(f) = nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$$

□

Theorem 6.6. *Let f be an $n(=2m)$ variable quadratic 2-MRS Boolean function generated by the monomial x_ax_b where $b-a$ is even and m is odd. Then f is balanced and its nonlinearity is given by $nl(f) = 2^{n-1} - 2^{\frac{3m+r}{2}-1}$ where $r = gcd(m, \frac{b-a}{2})$.*

Proof. Let $b - a = 2k$ and $m = n/2$ be odd then the Boolean function f is given by

$$f(x_0, x_1, ..., x_{n-1}) = x_ax_{a+2k} + x_{a+2}x_{a+2k+2} + ... + x_{a+n-2}x_{a+2k+n-2}$$

if we rename the variables as $x_a = y_0, x_{a+2} = y_1, ..., x_{a+n-2} = y_{m-1}$ then f is equivalent to

$$f \equiv y_0y_k + y_1y_{k+1} + ... + y_{m-1}y_{k+m-1}$$

Since m is odd $2k \not\equiv 0(mod m)$ hence all the terms in f are distinct. Define an m-variable Boolean function g whose algebraic normal form is same as f ie;

$$g(y_0, y_1, ..., y_{m-1}) = y_0y_k + y_1y_{k+1} + ... + y_{m-1}y_{k+m-1}$$

Let $r = gcd(m, k)$. Note that since m is odd $\frac{m}{r}$ is always odd. Hence by theorem 8 of [61] g is balanced and nonlinearity of g is given by $nl(g) = 2^{m-1} - 2^{\frac{m+r}{2}-1}$. Since f and g have the same ANF and g is balanced, f is also balanced.

Note that the maximum Walsh spectrum value of g is given by $max_a|W_g(a)| = 2^{\frac{m+r}{2}}$ as the nonlinearity of g is $nl(g) = 2^{m-1} - 2^{\frac{m+r}{2}-1}$. Hence $max_a|W_f(a)| = 2^{n-m}2^{\frac{m+r}{2}}$ so the nonlinearity of f is given by

$$nl(f) = 2^{n-1} - 2^{\frac{3m+r}{2}-1} \text{ and } wt(f) = 2^{n-1}$$

□

Theorem 6.7. *Let f be an $n(=2m)$-variable quadratic 2-MRS Boolean function generated by the monomial $x_a x_b$ where $b-a$ is even and equal to m then the weight and nonlinearity of the function f are same and is given by*

$$wt(f) = nl(f) = 2^{n-1} - 2^{\frac{3n}{4}-1}$$

Proof. Let $b-a = m$ then the function is $f(x_0, x_1, ..., x_{n-1}) = x_a x_{a+m} + x_{a+2}x_{a+m+2} + ... + x_{a+n-2}x_{a+m-2}$. If we rename the variables as $x_a = y_0, x_{a+2} = y_1, ..., x_{a+n-2} = y_{m-1}$ then f is equivalent to $f \equiv y_0 y_{\frac{m}{2}} + y_1 y_{\frac{m}{2}+1} + ... + y_{\frac{m}{2}-1} y_{m-1}$. Then by Lemma 5 of [61] weight of f is same as its nonlinearity and is given by

$$wt(f) = nl(f) = 2^{n-1} - 2^{\frac{3n}{4}-1}$$

□

Theorem 6.8. *Let f be an $n(=2m)$-variable quadratic 2-MRS Boolean function generated by the monomial $x_a x_b$ where $b-a(=2k)$ and m is even and let $r = gcd(m,k)$. Then the function f is balanced and has nonlinearity $2^{n-1} - 2^{\frac{3m+r}{2}-1}$ if $\frac{m}{r}$ is odd, else f has weight same as its nonlinearity and is given by*

$$wt(f) = nl(f) = 2^{n-1} - 2^{\frac{3m}{2}+r-1}$$

where $r = gcd(m,k)$

Proof. Let $b-a = 2k$ and $m = \frac{n}{2}$ be even then the Boolean function f is given by

$$f(x_0, x_1, ..., x_{n-1}) = x_a x_{a+2k} + x_{a+2}x_{a+2k+2} + ... + x_{a+n-2}x_{a+2k+n-2}$$

If we rename the variables as $x_a = y_0, x_{a+2} = y_1, ..., x_{a+n-2} = y_{m-1}$, then f is equivalent to

$$f \equiv y_0 y_k + y_1 y_{k+1} + ... + y_{m-1} y_{k+m-1}$$

since $k \neq \frac{m}{2}$ all the terms in f are distinct. Define an m-variable Boolean function g whose algebraic normal form is same as f ie;

$$g(y_0, y_1, ..., y_{m-1}) = y_0 y_k + y_1 y_{k+1} + ... + y_{m-1} y_{k+m-1}$$

Let $r = gcd(m, k)$, when $\frac{m}{r}$ is odd then by theorem 8 in [61] g is balanced and nonlinearity of g is given by $nl(g) = 2^{m-1} - 2^{\frac{m+r}{2}-1}$. Since f and g have same ANF and g is balanced f is also balanced. Note that since $nl(g) = 2^{m-1} - 2^{\frac{m+r}{2}-1}$ maximum absolute Walsh spectrum value of g is given by $max_a|W_g(a)| = 2^{\frac{m+r}{2}}$ hence $max_a|W_f(a)| = 2^{n-m}2^{\frac{m+r}{2}}$. So the nonlinearity of f is given by

$$nl(f) = 2^{n-1} - 2^{\frac{3m+r}{2}-1}$$

When $\frac{m}{r}$ is even by theorem 8 in [61] $wt(g) = nl(g) = 2^{m-1} - 2^{\frac{m}{2}+r-1}$. Since weight and nonlinearity of g is same the maximum absolute Walsh spectrum value of g given by $max_a|W_g(a)| = 2^{\frac{m}{2}+r}$ is attained at $a = 0$, hence $max_a|W_f(a)| = 2^{n-m}2^{\frac{m}{2}+r}$and it is attained at the point $a = 0$. Hence the weight of f is same as its nonlinearity and it is given by

$$wt(f) = nl(f) = 2^{n-1} - 2^{\frac{3m}{2}+r-1}$$

□

6.5 Rotation Symmetric S-boxes

An S-box is an important component used in different cryptographic primitives to achieve nonlinearity. An S-box [37] of order $m \times n$ is considered to be a mapping $s : \mathbb{F}_2^n \to \mathbb{F}_2^m$ which maps n-bit length inputs to m-bit length outputs. A cryptographically strong S-box is efficient in providing high nonlinearity if used properly in cryptographic primitives like stream ciphers, block ciphers and cryptographic hash functions. Most cryptosystems use S-boxes as the only nonlinear components, and hence the security of the entire system depends heavily on the cryptographic

properties of the S-boxes. Some of the widely accepted basic criterion for the selection of an S-box for cryptographic purposes are chosen by a tradeoff with high nonlinearity, Strict Avalanche Criterion (SAC), balancedness (or bijective), completeness, low differential uniformity, high algebraic immunity and robustness. The construction of appropriate S-boxes is one of the most challenging problems in the area of symmetric cryptography, and very few such constructions have emerged so far mostly using some power maps. The S-box of Advanced Encryption Standard (AES) uses the inverse function $s(a) = a^{-1}$ over $\mathbb{F}_{2^8}$, which provides fast implementation as the degree of the field is a power of 2, and achieves nice cryptographic properties. More specifically, for even n, the inverse function over $\mathbb{F}_{2^n}$ is differentially-4 uniform with the best known nonlinearity $2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$ and the maximum algebraic degree $n-1$. For odd n, there exist power maps having maximum nonlinearity $2^{n-1} - 2^{\lfloor \frac{n-1}{2} \rfloor}$, minimum differential uniformity 2, and high algebraic degree $\frac{n+1}{2}$.

Definition 6.9. *(Rotation symmetric S-box)*
An S-box S_B is rotation symmetric if

$$\rho_n^1(S_B(x_0, x_1, ..., x_{n-1})) = S_B(\rho_n^1(x_0, x_1, ..., x_{n-1}))$$

for all $(x_0, x_1, ..., x_{n-1}) \in F_2^n$.

Considering an S-box as a mapping $s : \mathbb{F}_2^n \to \mathbb{F}_2^m$ the S-boxes for which $(s(a))^2 = s(a^2)$ for any $a \in \mathbb{F}_2^n$ can be regarded as rotation symmetric by mapping the field elements to their coordinates in normal basis for $\mathbb{F}_{2^n}$. In 2008 Vincent Rijmen et al.[79] showed that the S-boxes generated from the polynomials over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$, and exponentiations over $\mathbb{F}_{2^n}$ are linearly equivalent to rotation symmetric S-boxes. Hence, most of the S-box constructions can be considered as rotation symmetric S-boxes, which demonstrates the fact that this class of S-boxes contains cryptographically desirable S-boxes to be used in practical cryptosystems.

Consider the 8-bit to 8-bit S-box given in table 6.1. A representative element from each of the 36 orbits of the S-box is chosen and their corresponding output from

Table 6.1: Reduced Truth Table of S-box

Input	Output
[0, 0, 0, 0, 0, 0, 0, 0]	[1, 1, 1, 1, 1, 1, 1, 1]
[0, 0, 0, 0, 0, 0, 0, 1]	[0, 0, 1, 1, 0, 1, 0, 1]
[0, 0, 0, 1, 0, 0, 0, 1]	[0, 1, 1, 1, 0, 1, 1, 1]
[0, 0, 0, 0, 1, 0, 0, 1]	[0, 1, 1, 0, 0, 0, 0, 1]
[0, 0, 0, 0, 0, 1, 0, 1]	[1, 1, 0, 1, 0, 0, 1, 1]
[0, 0, 1, 0, 0, 1, 0, 1]	[0, 0, 1, 0, 1, 1, 1, 0]
[0, 0, 0, 1, 0, 1, 0, 1]	[0, 1, 0, 0, 1, 0, 1, 1]
[0, 1, 0, 1, 0, 1, 0, 1]	[0, 1, 0, 1, 0, 1, 0, 1]
[0, 0, 0, 0, 0, 0, 1, 1]	[0, 0, 0, 0, 0, 1, 0, 1]
[0, 1, 0, 0, 0, 0, 1, 1]	[1, 1, 0, 0, 1, 0, 0, 1]
[0, 0, 1, 0, 0, 0, 1, 1]	[0, 0, 1, 1, 0, 0, 0, 1]
[0, 0, 0, 1, 0, 0, 1, 1]	[0, 1, 1, 1, 1, 1, 1, 0]
[0, 1, 0, 1, 0, 0, 1, 1]	[1, 1, 1, 0, 1, 1, 0, 0]
[0, 0, 1, 1, 0, 0, 1, 1]	[0, 1, 0, 0, 0, 1, 0, 0]
[0, 0, 0, 0, 1, 0, 1, 1]	[0, 0, 0, 0, 0, 0, 1, 1]
[0, 1, 0, 0, 1, 0, 1, 1]	[0, 0, 1, 1, 1, 0, 1, 0]
[0, 0, 1, 0, 1, 0, 1, 1]	[0, 1, 0, 1, 1, 1, 1, 1]
[0, 0, 0, 1, 1, 0, 1, 1]	[0, 1, 1, 0, 0, 1, 0, 0]
[0, 1, 0, 1, 1, 0, 1, 1]	[0, 0, 0, 0, 1, 1, 1, 1]
[0, 0, 0, 0, 0, 1, 1, 1]	[1, 0, 1, 0, 0, 1, 0, 0]
[0, 1, 0, 0, 0, 1, 1, 1]	[0, 0, 1, 0, 1, 0, 1, 1]
[0, 0, 1, 0, 0, 1, 1, 1]	[0, 1, 1, 0, 1, 1, 1, 1]
[0, 1, 1, 0, 0, 1, 1, 1]	[1, 1, 0, 1, 1, 1, 0, 0]
[0, 0, 0, 1, 0, 1, 1, 1]	[0, 1, 1, 1, 1, 0, 0, 1]
[0, 1, 0, 1, 0, 1, 1, 1]	[1, 1, 1, 0, 0, 0, 1, 1]
[0, 0, 1, 1, 0, 1, 1, 1]	[1, 1, 1, 0, 1, 1, 1, 1]
[0, 1, 1, 1, 0, 1, 1, 1]	[0, 0, 1, 1, 0, 0, 1, 1]
[0, 0, 0, 0, 1, 1, 1, 1]	[0, 0, 0, 0, 0, 1, 1, 1]
[0, 1, 0, 0, 1, 1, 1, 1]	[0, 1, 0, 0, 0, 0, 1, 0]
[0, 0, 1, 0, 1, 1, 1, 1]	[0, 0, 0, 0, 1, 1, 0, 1]
[0, 1, 1, 0, 1, 1, 1, 1]	[0, 1, 1, 0, 1, 1, 0, 1]
[0, 0, 0, 1, 1, 1, 1, 1]	[0, 1, 0, 1, 0, 1, 1, 1]
[0, 1, 0, 1, 1, 1, 1, 1]	[0, 1, 0, 0, 0, 1, 0, 1]
[0, 0, 1, 1, 1, 1, 1, 1]	[0, 0, 0, 0, 0, 0, 1, 0]
[0, 1, 1, 1, 1, 1, 1, 1]	[1, 1, 0, 0, 0, 1, 1, 0]
[1, 1, 1, 1, 1, 1, 1, 1]	[0, 0, 0, 0, 0, 0, 0, 0]

the S-box S_B is given in the table 6.1. The output corresponding to an arbitrary input $(x_0, x_1, ..., x_7) \in F_2^8$ of the S-box S_B is worked out as $S_B(x) = \rho_8^k(S_B(r))$ for some fixed k, $1 \leq k \leq 8$, such that $\rho_8^k(x) = r$, where r is one of the representatives of the 36 orbits of the S-box given in input column of table 6.1. This helps us to

greatly reduce the 256 bytes S-box lookup table to 72 bytes reduced lookup table by introducing a negligibly small computation as defined above.

Definition 6.10. *(Strict Avalanche Criterion)*
Let $S_B(x) = (f_1(x), f_2(x), ..., f_n(x))$ from F_2^n to F_2^n be a multiple output Boolean function. $S_B(x)$ satisfies Strict Avalanche Criterion (SAC) if for all $\alpha \in F_2^n$ with $wt(\alpha) = 1$, $wt(f_i(x \oplus \alpha) \oplus f_i(x)) = 2^{n-1}$, $(1 \leq i \leq n)$.

The 8-bit rotation symmetric S-box given in table 6.1 has the following properties: nonlinearity 102, bijective, complete, robustness 0.96875, SAC (refer table 6.2), differential uniformity 8. Each of the eight component Boolean functions associated with the S-box has algebraic immunity 4 and nonlinearity 106. These properties form a measure of security against linear, differential and algebraic cryptanalysis.

Table 6.2: SAC of S-box

Input Error Vector ↓	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
[0, 0, 0, 0, 0, 0, 0, 1]	112	120	132	144	136	120	124	140
[0, 0, 0, 0, 0, 0, 1, 0]	140	112	120	132	144	136	120	124
[0, 0, 0, 0, 0, 1, 0, 0]	124	140	112	120	132	144	136	120
[0, 0, 0, 0, 1, 0, 0, 0]	120	124	140	112	120	132	144	136
[0, 0, 0, 1, 0, 0, 0, 0]	136	120	124	140	112	120	132	144
[0, 0, 1, 0, 0, 0, 0, 0]	144	136	120	124	140	112	120	132
[0, 1, 0, 0, 0, 0, 0, 0]	132	144	136	120	124	140	112	120
[1, 0, 0, 0, 0, 0, 0, 0]	120	132	144	136	120	124	140	128

In 2012 Selçuk Kavut [77] extended the definition of k-rotation symmetric Boolean functions to the multi output case and described the generalized classes of k-rotation symmetric S-boxes as the polynomials of $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^k}$, where k divides n. They defined the generalized k-rotation symmetric S-boxes as the functions which satisfy $(s(a))^{2^k} = s(a^{2^k})$. Notice that if $k = 1$, the resulting class corresponds to conventional rotation symmetric S-boxes, whereas if $k = n$, the generalized k-rotation symmetric S-boxes cover the entire space of $n \times n$ S-boxes.