Rotation Symmetric Boolean Functions – Count and Cryptographic Properties

Pantelimon Stănică *
Department of Mathematics
Auburn University Montgomery,
Montgomery, AL 36124-4023, USA
E-mail: stanica@strudel.aum.edu

Subhamoy Maitra
Applied Statistics Unit,
Indian Statistical Institute
203 B. T. Road, Calcutta 700 108, INDIA
E-mail: subho@isical.ac.in

Abstract

In 1999, Pieprzyk and Qu presented *rotation symmetric* (*RotS*) functions as components in the rounds of hashing algorithm. Later, in 2002, Cusick and Stănică presented further advancement in this area. This class of Boolean functions are invariant under circular translation of indices. In this paper, using Burnside's lemma we prove that the number of n-variable rotation symmetric Boolean functions is 2^{g_n}, where $g_n = \frac{1}{n}\sum_{t|n}\phi(t)\,2^{\frac{n}{t}}$, and $\phi(.)$ is the Euler *phi*-function. Moreover, we find the number of short and long cycles of elements in $\mathbf{Z}_2^n$ having fixed weight, under the *RotS* action. As a consequence we obtain the number of homogeneous *RotS* functions having algebraic degree w. Our results make the search space of *RotS* functions much reduced and we successfully analyzed important cryptographic properties of such functions by executing computer programs. We found that there are exactly $8, 48$, and 15104, *RotS* bent functions on $4, 6$, and 8 variables respectively. Experimental results up to 10 variables show that there is no homogeneous rotation symmetric bent function with degree > 2. Further, we studied the *RotS* functions on $5, 6, 7$ variables for correlation immunity and propagation characteristics and found some functions with very good cryptographic properties which were not known earlier.

Keywords: Rotation Symmetric Boolean Functions, Enumeration, Correlation Immunity, Resiliency, Algebraic Degree, Nonlinearity, Autocorrelation.

1 Introduction

In [9], Pieprzyk and Qu studied some functions, which they called *rotation symmetric* (*RotS*) as components in the rounds of a hashing algorithm. This is a desirable property when efficient evaluation of the function is important, for instance in the implementation of MD4, MD5 or HAVAL, since one can reuse evaluations from previous iterations. It turns out that a degree 2 *RotS* function on n variables takes $\frac{3n-1}{2} + 6(m-1)$ operations (additions and multiplications) to evaluate in m consecutive rounds of a hashing algorithm. In [7] the authors showed how to break in less than 20 mili-seconds a block cipher that employs quadratic Boolean functions as its S-boxes even if it is provably secure against linear and differential attacks. This suggests that one should employ higher degree functions in cryptographic algorithms. Moreover, it is clear that to protect from linear and differential cryptanalysis, one needs functions with high nonlinearity. The study started by Pieprzyk and Qu [9] on the 2-degree *RotS* functions was continued in [5],

*Also associated with the Institute of Mathematics of Romanian Academy, Bucharest, Romania.

the authors investigating these in the even dimensions. It has been shown that the truth table of an n-variable degree 2 *RotS* function can be displayed using only $2^{n-3}-2$ operations (additions and multiplications) as opposed to $\lfloor \frac{3n-1}{2} \rfloor 2^n$, using the normal form. In [5] some results about the weights and nonlinearity of degree 3 *RotS* functions have been proved and it was conjectured that the weight and nonlinearity of any degree 3 (homogeneous) *RotS* function are equal. It has been shown [5] that the truth table of a degree 3 *RotS* function can be displayed using only $2^{n-2}+2^{n-4}+2^{n-5}-3\cdot 2^2$ operations (additions and multiplications).

It is clear that there are 2^{2^n} Boolean functions on n variables and under no circumstances (with current computational power) it is possible to search them exhaustively for $n \geq 7$ to check some desired property. Thus before analyzing the *RotS* Boolean functions the immediate question is: how many rotation symmetric functions are there? We show that the number of rotation symmetric Boolean functions is a very small fraction of the total number of Boolean functions and it is possible to search the space with much better efficiency.

Before proceeding further let us present some introductory material for better understanding. Let V_n be the vector space of dimension n over the two element field $\mathbf{Z}_2$. Let $x_i \in \{0,1\}$ for $1 \leq i \leq n$. For $1 \leq k \leq n$, we define

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

Let $(x_1, x_2, \ldots, x_{n-1}, x_n) \in V_n$. Then we extend the definition as

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

x_4	x_3	x_2	x_1	f
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	1
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	1
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

no.	x_4	x_3	x_2	x_1	f
1	0	0	0	0	0
2	0	0	0	1	1
2	0	0	1	0	1
3	0	0	1	1	0
2	0	1	0	0	1
4	0	1	0	1	0
3	0	1	1	0	0
5	0	1	1	1	1
2	1	0	0	0	1
3	1	0	0	1	0
4	1	0	1	0	0
5	1	0	1	1	1
3	1	1	0	0	0
5	1	1	0	1	1
5	1	1	1	0	1
6	1	1	1	1	1

Table 1: Truth table of Boolean functions.

A Boolean function on n variables may be viewed as a mapping from V_n into V_1. We interpret a Boolean function $f(x_1, \ldots, x_n)$ as the output column of its *truth table*, i.e., a binary string of length 2^n, $f = [f(0,0,\ldots,0),\ f(1,0,\ldots,0), f(0,1,\ldots,0), \ldots, f(1,1,\ldots,1)]$. In Table 1 we present truth tables of 4-variable Boolean functions.

Definition 1. *A Boolean function f is RotS if and only if for any $(x_1, \ldots, x_n) \in V_n$,*

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

for any $1 \leq k \leq n$.

Note that there are 2^n different input values corresponding to a function. From the above definition, it is clear that for *RotS* functions, the function f possesses the same value corresponding to each of the subsets generated from the rotational symmetry. As example, for $n=4$, one gets the following partitions :

$$\{(0,0,0,0)\},$$
$$\{(0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0)\},$$
$$\{(0,0,1,1),(0,1,1,0),(1,0,0,1),(1,1,0,0)\},$$
$$\{(0,1,0,1),(1,0,1,0)\},$$
$$\{(0,1,1,1),(1,0,1,1),(1,1,0,1),(1,1,1,0)\},$$
$$\{(1,1,1,1)\}.$$

Therefore, there are 6 different subsets which partition the 16 input patterns and any 4-variable *RotS* Boolean function can have a specific value corresponding to each subset. Thus there are $2^6 = 64$ rotation symmetric functions on 4 variables. In Table 1, the left one is a function which is not *RotS* , whereas, the right one is a *RotS* function (each different subset is numbered). Note that there are 6 different subsets and two of them are of size 1, one is of size 2 and the rest three are of size 4.

Let us denote

$$G_n(x_1, \ldots, x_n) = \{\rho_n^k(x_1, \ldots, x_n), \text{ for } 1 \leq k \leq n\},$$

that is, the orbit of $(x_1, \ldots, x_n)$ under the action of ρ_n^k, $1 \leq k \leq n$. It is clear that $G_n(x_1, \ldots, x_n)$ generates a partition in the set V_n. Let g_n be the number of such partitions. As example $g_4 = 6$. Given $(x_1, \ldots, x_n)$, a function is *RotS* if it takes the same value for all the inputs in $G_n(x_1, \ldots, x_n)$. It is clear that there are 2^{g_n} number of n-variable *RotS* Boolean functions. From Burnside's lemma, we get that $g_n = \frac{1}{n}\sum_{t|n} \phi(t)\, 2^{\frac{n}{t}}$ (see Section 2). In Table 2, we present the first few values of g_n.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
g_n	2	3	4	6	8	14	20	36	60	108	188	352	632	1182	2192	4116

Table 2: The values of g_n, $1 \leq n \leq 16$.

For binary strings S_1, S_2 of the same length λ, we denote by $\#(S_1 = S_2)$ (respectively, $\#(S_1 \neq S_2)$), the number of places where S_1 and S_2 are equal (respectively, unequal). The *Hamming distance* between S_1, S_2 is $d(S_1, S_2) = \#(S_1 \neq S_2)$. We will also use the notation $wd(S_1, S_2) = \#(S_1 = S_2) - \#(S_1 \neq S_2)$. Note that, $wd(S_1, S_2) = \lambda - 2\,d(S_1, S_2)$. Also, the *Hamming weight*, $wt(S)$, or simply the weight of a binary string S is the number of ones in S. An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0's and 1's (i.e., $wt(f) = 2^{n-1}$).

Let us denote the addition operator over $GF(2)$ by $+$. An n-variable Boolean function $f(x_1, \ldots, x_n)$ can be seen as a multivariate polynomial over $GF(2)$. More precisely, $f(x_1, \ldots, x_n)$ can be written as $a_0 + \sum_{i=1}^n a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \ldots + a_{12\ldots n} x_1 x_2 \ldots x_n$, where the coefficients $a_0, a_i, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. This representation of f is called the *algebraic normal form* (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree*, or simply the degree of f. A Boolean function is said to be homogeneous if its ANF contains terms of the same degree only.

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 set of all n-variable affine (respectively linear) functions is denoted by $A(n)$ (respectively $L(n)$). The *nonlinearity* of an n-variable function f is $nl(f) = min_{g \in A(n)}(d(f, g))$, i.e., the distance from the set of all n-variable affine functions.

Clearly one can extend ρ_n on monomials of the form $x_{i_1} x_{i_2} \ldots x_{i_l}$. Let us take an example of 4-variable *RotS* function. If the term $x_1 x_2 x_3$ is present in the ANF, then the terms $x_2 x_3 x_4, x_3 x_4 x_1, x_4 x_1 x_2$ must be present in the ANF. Thus we can naturally extend the notation as $\rho_n^k(x_{i_1}x_{i_2}\ldots x_{i_l}) = \rho_n^k(x_{i_1})\rho_n^k(x_{i_2})\ldots\rho_n^k(x_{i_l})$. Similarly, in this case $G_n(x_{i_1}x_{i_2}\ldots x_{i_l}) = \{\rho_n^k(x_{i_1}x_{i_2}\ldots x_{i_l}),\ \text{for } 1 \le k \le n\}$.

We select the representative element of $G_n(x_{i_1}x_{i_2}\ldots x_{i_l})$ as the lexicographically first element. As example, the representative element of $\{x_1x_2x_3,\ x_2x_3x_4,\ x_3x_4x_1,\ x_4x_1x_2\}$ is $x_1x_2x_3$. Note that it is also clear that the term x_1 will always exist in the lexicographically first element (the representative element).

We now define the *short algebraic normal form* (SANF) of a *RotS* function. A *RotS* function $f(x_1,\ldots,x_n)$ can be written as

$$a_0 + a_1x_1 + \sum a_{1j}x_1x_j + \ldots + a_{12\ldots n}x_1x_2\ldots x_n,$$

where the coefficients $a_0, a_1, a_{1j}, \ldots, a_{12\ldots n} \in \{0,1\}$, and the existence of a representative term $x_1x_{i_2}\ldots x_{i_l}$ implies the existence of all the terms from $G_n(x_1x_{i_2}\ldots x_{i_l})$ in the ANF. This representation of f is called the *short algebraic normal form* (SANF) of f. Note that the number of terms in each summation ($\sum$) corresponding to same degree terms depends on the number of short and long cycles.

As example consider the ANF of a 4-variable *RotS* Boolean function $x_1 + x_2 + x_3 + x_4 + x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2$. Its SANF is $x_1 + x_1x_2x_3$.

As we have already mentioned, a Boolean function is said to be homogeneous if its algebraic normal form contains terms of same degree only. It is an important question to settle the enumeration of homogeneous *RotS* functions, which we present in the next section (Subsection 2.2). Further this helps us in reducing the search space for *RotS* functions and we develop computer programs to explore bent functions and other cryptographically significant Boolean functions in this set (see Section 3). Using the computer search in a reduced space, we found the exact count of 8, 48, and 15104, *RotS* bent functions on 4, 6, and 8 variables respectively. Homogeneous bent functions have recently got a lot of attention in literature [2, 3, 11, 16]. It is interesting to note that we could not find any homogeneous *RotS* bent functions having degree > 2 up to 10 variables.

It is clear that cryptographically significant *RotS* functions are of interest [9, 5], though such functions could not be constructed yet. Our attempt to search the cryptographically significant Boolean functions on 5, 6 and 7 variables produced extremely encouraging results (see Section 3 for relevant definitions). We found 480 *RotS* functions on 7 variables which possess resiliency of order 1, propagation characteristics of order 1, nonlinearity 56, algebraic degree 4 and maximum absolute value in autocorrelation spectra 16. Also we found 72 *RotS* functions on 7 variables which possess resiliency of order 2, nonlinearity 56, algebraic degree 4 and maximum absolute value in autocorrelation spectra 16. Functions with such optimized properties were not known earlier.

2 Enumeration of Rotation Symmetric Boolean Functions

We start this section with some basic technical discussion. It is clear that $|G_n(x_1,\ldots,x_n)| \le n$. For the case $|G_n(x_1,\ldots,x_n)| = n$, we call that the elements of $G_n(x_1,\ldots,x_n)$ form a long cycle, which is of length n. On the other hand, if $|G_n(x_1,\ldots,x_n)| < n$, we call it a short cycle, which is of length strictly less than n. As example, $G_4(1,0,0,0)$, $G_4(1,1,0,0)$, $G_4(1,1,1,0)$ are long cycles (each of size 4), whereas, $G_4(0,0,0,0), G_4(1,1,1,1)$ (each of size 1) and $G_4(1,0,1,0)$ (of size 2) are short cycles. Note that $|G_n(0,\ldots,0)| = |G_n(1,\ldots,1)| = 1$, for any $n \ge 1$. For $n = 1$, $G_1(0), G_1(1)$ are two long cycles. However, for $n > 1$, $G_n(0,\ldots,0), G_n(1,\ldots,1)$ are always short cycles.

It turns out that the sequence g_n counts also the number of n-bead necklaces with 2 colors when turning over is not allowed, or output sequences from a simple n-stage cycling shift register, or binary irreducible polynomials whose degree divides n (see [15]). In the proof of our first result, we need Burnside's lemma (which in fact was discovered by Frobenius).

Lemma 2 (Burnside's lemma). *Let G be a group of permutations acting on a set S. Then the number of orbits induced on S is given by $\frac{1}{|G|}\sum_{\pi\in G}|fix_S(\pi)|$, where $fix_S(\pi)=\{x\in S\,|\,\pi(x)=x\}$.*

Theorem 3. $g_n = \frac{1}{n}\sum_{t|n}\phi(t)\,2^{n/t}$*, where $\phi(t)$ is Euler's phi-function.*

Proof. For convenience, we provide here a proof (see also [15]). Here $G=\{\rho_n^1,\ldots,\rho_n^n\}$ and $S=\{0,1\}^n$. To use Burnside's lemma we need to find the number of fixed points of ρ_n^i, $i=1,\ldots,n$. The number of permutation cycles of ρ_n^i is $\gcd(n,i)$, each of them of length $\frac{n}{\gcd(n,i)}$. Observe that ρ_n^i has order $\frac{n}{\gcd(n,i)}$. Since, to be fixed by ρ_n^i, each input cycle must consist of all 0's or all 1's, we get that the number of fixed points of ρ_n^i is $2^{\gcd(n,i)}$. Applying Burnside's lemma we obtain, $g_n=\frac{1}{n}\sum_{i=1}^n 2^{\gcd(n,i)}=\frac{1}{n}\sum_{k|n}\sum_{i,\,\gcd(n,i)=k}^n 2^k=\frac{1}{n}\sum_{k|n}2^k\sum_{j,\,\gcd(n/k,j)=1}1=\frac{1}{n}\sum_{k|n}\phi\left(\frac{n}{k}\right)2^k=\frac{1}{n}\sum_{t|n}\phi(t)\,2^{\frac{n}{t}}$. ☐

The number of rotation symmetric functions of n variables is 2^{g_n}. There are two groups $G_n(0,\ldots,0)$, $G_n(1,\ldots,1)$ of size 1. Moreover, we know that all other groups have size $\le n$. There are in total 2^n tuples in V_n. Thus apart from the $(0,\ldots,0)$, $(1,\ldots,1)$ tuples, there are at least $\lceil\frac{2^n-2}{n}\rceil$ groups. Hence, $g_n\ge\frac{2^n+2n-2}{n}$. Further, for n prime, $g_n=\frac{2^n+2n-2}{n}$.

Corollary 4. *For prime p, $g_{p^a}=p^{-a}\left(2^{p^a}+\sum_{i=1}^{a}(p^i-p^{i-1})2^{p^{a-i}}\right)$.*

Proof. Take $n=p^a$. Any divisor of such an n is of the form p^i, $0\le i\le n$. Moreover, $\phi(p^i)=p^i-p^{i-1}$. Applying Theorem 3 we obtain $g_{p^a}=p^{-a}\left(2^{p^a}+\sum_{i=1}^{a}(p^i-p^{i-1})2^{p^a/p^i}\right)$, which gives the corollary (the first term corresponds to the divisor $t=1$ of n). ☐

2.1 Enumeration of long cycles

Concentrate on $G_n(x_1,\ldots,x_n)$, where $G_n(x_1,\ldots,x_n)$ contains *exactly* n elements. Let h_n be the number of such length n subsets, i.e., the number of long cycles. Clearly $h_n<g_n$. We will provide a formula for h_n.

Let ω_n be the number of prime factors of n, and $n=p_1^{a_1}\cdots p_{\omega_n}^{a_{\omega_n}}$. First we need a few technical results.

Lemma 5. *If $\gcd(i,n)=d$, then the fixed points of ρ_n^i are exactly the fixed points of ρ_n^d.*

Proof. Since, $\gcd(n,i)=\gcd(n,d)=d$, ρ_n^i and ρ_n^d have the same number of fixed points. Therefore, it suffices to show that the fixed points of ρ_n^d are also fixed points of ρ_n^i. Take $(x_1,\ldots,x_n)$ a fixed point of ρ_n^d. Let $i=di'$. We have

$$\rho_n^i(x_1,\ldots,x_n)=\rho_n^{di'}(x_1,\ldots,x_n)=\rho_n^d(\rho_n^d(\ldots\rho_n^d(x_1,\ldots,x_n)\ldots))=(x_1,\ldots,x_n),$$

where the composition contains i' number of ρ_n^d operations. Thus, $(x_1,\ldots,x_n)$ is a fixed point of ρ_n^i. ☐

Lemma 6. *If $a\le b$ and $p\,|\,n$, then the fixed points of $\rho_n^{p^a}$ are among the fixed points of $\rho_n^{p^b}$.*

Proof. Take $(x_1, \ldots, x_n)$ a fixed point of $\rho_n^{p^a}$. We need to show that it is a fixed point of $\rho_n^{p^b}$, as well. This follows from $\rho_n^{p^b}(x_1, \ldots, x_n) = \rho_n^{p^a}(\ldots \rho_n^{p^a}(x_1, \ldots, x_n) \ldots) = (x_1, \ldots, x_n)$, where the composition contains $b - a$ terms. $\square$

Let $p \neq q$ be prime divisors of n, and a, b arbitrary integers. Denote F_{p^a}, F_{q^b}, the set of fixed points of $\rho_n^{p^a}$, respectively, $\rho_n^{q^b}$.

Lemma 7. *We have* $F_{p^a} \bigcap F_{q^b} = \{(0, \ldots, 0), (1, \ldots, 1)\}$.

Proof. We know ρ_n has only two obvious fixed points. Assume that $(x_1, \ldots, x_n)$ is a fixed point in the intersection, which is neither $(0, \ldots, 0)$, nor $(1, \ldots, 1)$. If $\rho_n^{q^b}(x_1, \ldots, x_n) = (x_1, \ldots, x_n)$, then $\rho_n^{-q^b}(x_1, \ldots, x_n) = (x_1, \ldots, x_n)$. Since $p \neq q$, then $\gcd(p^a, q^b) = 1$, therefore there exist some integers A, B, such that $Ap^a + Bq^b = 1$. Assume $A > 0, B < 0$. Thus, $\rho_n^1(x_1, \ldots, x_n) = \rho_n^{Ap^a + Bq^b}(x_1, \ldots, x_n) = \rho_n^{Ap^a}(\rho_n^{Bq^b}(x_1, \ldots, x_n)) = (x_1, \ldots, x_n)$, a contradiction. $\square$

Theorem 8. *We have (i)* $h_1 = 2$,

(ii) If $n = p^a$, *p prime, then* $h_{p^a} = \dfrac{1}{n} \sum_{d|n} \phi(d)\, 2^{n/d} - \sum_{i=1}^{a-1} \dfrac{2^{p^i} - 2^{p^{i-1}}}{p^i} - 2$. *In particular, if* $a = 1$, $h_p = \dfrac{2^p - 2}{p}$.

(iii) Let $n = p_1^{a_1} \cdots p_{\omega_n}^{a_{\omega_n}}$, $p_i \neq p_j$ *be the prime factorization. Then* $h_n = \dfrac{1}{n} \sum_{d|n} \phi(d)\, 2^{n/d} - \sum_{i=1}^{\omega_n} \sum_{j=1}^{a_i} \dfrac{2^{p_i^j} - 2^{p_i^{j-1}}}{p_i^j} - 2$, *if* $\omega_n \geq 2$.

Proof. It is easy to see that $h_1 = 2$. This is the ***Case*** *(i)*. Note that $G_n(x_1, \ldots, x_n)$ is a short cycle, if and only if there is some proper divisor $d \,|\, n$, such that $(x_1, \ldots, x_n)$ is a fixed point for ρ_n^d. From the previous lemmata, it suffices to consider d a power of a prime.
Case *(ii)*. $\omega_n = 1$, therefore $n = p^a$, for some integer a and prime p. We count the short cycles for $\rho_n^{p^a}$ by looking at the fixed points of $\rho_n^{p^i}$, $0 \leq i < a$. Obviously, we have fixed points only for $\rho_n^{p^i}$, $0 \leq i < a$, which are *all* fixed points for $\rho_n^{p^{a-1}}$, also.

But a short cycle under $\rho_n^{p^a}$ is a long cycle under $\rho_n^{p^i}$, for some $0 \leq i \leq a-1$. To find the long cycles under $\rho_n^{p^i}$, we take the fixed points of $\rho_n^{p^i}$, which are not fixed points of $\rho_n^{p^{i-1}}$ and divide by the length p^i of a long cycle under $\rho_n^{p^i}$. Recall that the number of fixed points of $\rho_n^{p^i}$ is 2^{p^i}. We get that the number of short cycles of ρ_n is $2 + \sum_{i=1}^{a-1} \dfrac{2^{p^i} - 2^{p^{i-1}}}{p^i}$.

Case *(iii)*. $\omega_n > 1$. Since the number of cycles of $\rho_n^{p_i^{a_i}}$ (by Lemma 7, these cycles are not fixed by any other $\rho_n^{p_j^{a_j}}, j \neq i$) is $\sum_{j=1}^{a_i} \dfrac{2^{p_i^j} - 2^{p_i^{j-1}}}{p_i^j}$, we obtain that the total number of short cycles is $2 + \sum_{i=1}^{\omega_n} \sum_{j=1}^{a_i} \dfrac{2^{p_i^j} - 2^{p_i^{j-1}}}{p_i^j}$. The number of short cycles is to be subtracted. Hence the proof of the theorem. $\square$

2.2 Homogeneous Rotation Symmetric Boolean functions

We noted already that for *RotS* Boolean functions, if the term $x_{i_1}x_{i_2}\dots x_{i_m}$ is present, then all the distinct terms of the form $\rho_n^j(x_{i_1}x_{i_2}\dots x_{i_m})$ are also present for $1 \le j < n$. Hence, for *RotS* functions, it is clear that some monomials of the same degree either appear or do not appear at the same time. Now we concentrate on monomials of the same degree. We introduce some notations which are related to the weight of the binary strings. First consider $G_n(x_1,\dots,x_n)$, where $wt(x_1,\dots,x_n)$ is exactly w. Note that in this way we get a partition over the n bit binary strings of weight w (total number $\binom{n}{w}$). Let us consider that the number of such partitions is $g_{n,w}$. Moreover, let $h_{n,w}$ be the number of distinct sets $G_n(x_1,\dots,x_n)$, where $wt(x_1,\dots,x_n) = w$ and $|G_n(x_1,\dots,x_n)| = n$, that is, the number of long cycles of weight w. Clearly, $h_{n,w} < g_{n,w}$.

We will write $k|'m$, if k, $(1 < k \le m)$ is a proper divisor of m.

Theorem 9. *We have*

(*i*) $g_{n,w} = \frac{1}{n}\binom{n}{w}$, *if* $gcd(n,w) = 1$. *Also,* $g_{n,0} = g_{n,n} = 1$.

(*ii*) $g_{n,w} = \frac{1}{n}\left(\binom{n}{w} - \sum_{k|'gcd(n,w)} \frac{n}{k}\cdot h_{\frac{n}{k},\frac{w}{k}}\right) + \sum_{k|'gcd(n,w)} h_{\frac{n}{k},\frac{w}{k}}$, *if* $w < n$.

Proof. First, we make the observation that $g_{n,w}$ is the sum between the number of long and short cycles. Obviously, $x = (x_1,\dots,x_n)$ is part of a short cycle, if and only if there is a minimal block $b = [x_1,x_2,\dots,]$ which by repeating itself (say, k times) covers x, that is $x = bbb\dots$. Furthermore, k divides w, so the weight of b is $\frac{w}{k}$. Since x is covered by concatenating k copies of b, it follows that k divides n, as well. This gives that there can not be any short cycle if $\gcd(n,w) = 1$ and hence we obtain the first claim of (i). If $w = 0$ (respectively $w = n$), then the only element x of such a weight is $(0,\dots,0)$ (respectively $(1,\dots,1)$), so $g_{n,0} = g_{n,n} = 1$. The proof of (i) is completed.

Assume $1 < w < n$. Using the same observation as above, we note that $(x_1,\dots,x_n)$ is part of a short cycle under g_n, if and only if there is a minimal block b, of length n/k, where $k\,|'\gcd(n,w)$, which renders x by concatenation of k copies of b. Since b is minimal, then it must be a full cycle under $g_{\frac{n}{k}}$, of weight $\dfrac{w}{k}$. Thus,

$$\#\text{ short cycles} = \sum_{k\,|'\gcd(n,w)} h_{\frac{n}{k},\frac{w}{k}}. \tag{1}$$

Let L (respectively S) be the sets of elements in $\mathbf{Z}_2^n$ of weight w, which are part of long (respectively short) cycles. Recall that the total number of elements of weight w is $\binom{n}{w}$. Therefore, $|L| = \binom{n}{w} - |S|$. The number of long cycles is $\frac{1}{n}|L|$. Moreover, each short cycle under g_n of weight w is the concatenation of k copies (for some value of $k\,|'\gcd(n,w)$) of a long cycle under $g_{\frac{n}{k}}$ of weight $\frac{w}{k}$. Since in each long cycle under $g_{\frac{n}{k}}$ of weight $\dfrac{w}{k}$ there are $\dfrac{n}{k}$ elements, it follows that

$$\#\text{ long cycles} = \frac{1}{n}\binom{n}{w} - \frac{1}{n}\sum_{k\,|'\gcd(n,w)} \frac{n}{k}\cdot h_{\frac{n}{k},\frac{w}{k}}. \tag{2}$$

Putting together 1 and 2, we obtain (ii). $\square$

Recall that $g_{n,w}$ is the number of distinct cycles of weight w. This means that the degree w monomials can be divided in $g_{n,w}$ different cycles. We obtain

Corollary 10. *Consider n-variable RotS Boolean functions. The number of (i) degree w homogeneous functions is $2^{g_{n,w}}-1$, (ii) the number of degree w functions is $(2^{g_{n,w}}-1)2^{\sum_{i=0}^{w-1} g_{n,i}}$ and (iii) the number of functions with degree at most w is $2^{\sum_{i=0}^{w} g_{n,i}}$.*

The result of Corollary 10 will be used in Subsection 3.1 as it reduces the search space of *RotS* bent functions.

Let us consider the case for $w=2$. If n is odd, then $g_{n,2}=\dfrac{n-1}{2}$. If n is even, $g_{n,2}=\dfrac{1}{n}\left(\binom{n}{2}-\dfrac{n}{2}\cdot h_{\frac{n}{2},1}\right)+h_{\frac{n}{2},1}$. Since $h_{\frac{n}{2},1}=1$, we get $g_{n,2}=\dfrac{n}{2}$. Thus there are $2^{\lfloor\frac{n}{2}\rfloor}$ homogeneous quadratic *RotS* Boolean functions.

Let us consider the case of degree $w=3$. If 3 does not divide n, then $g_{n,3}=\dfrac{1}{n}\binom{n}{3}=\dfrac{(n-1)(n-2)}{6}$. If n is divisible by 3, then $g_{n,3}=\dfrac{1}{n}\left(\binom{n}{3}-\dfrac{n}{3}\cdot h_{\frac{n}{3},1}\right)+h_{\frac{n}{3},1}$. Now $h_{\frac{n}{3},1}=1$. Hence, $g_{n,3}=\dfrac{1}{n}\left(\binom{n}{3}-\dfrac{n}{3}\right)+1=\dfrac{n(n-3)}{6}+1$. The number of homogeneous degree 3 *RotS* functions is $2^{g_{n,3}}$.

2.3 Solving the recurrence relation

Since $g_{n,w}$ depends on values of $h_{\cdot,\cdot}$ we shall display now an exact formula for these values. Let us recapitulate the equation 2 in the proof of Theorem 9, which is the recurrence relation for $h_{n,w}$.

$$h_{n,w}=\frac{1}{n}\binom{n}{w}-\frac{1}{n}\sum_{k\,|'\,\gcd(n,w)}\frac{n}{k}\cdot h_{\frac{n}{k},\frac{w}{k}}. \tag{3}$$

Let n,w be such that $\gcd(n,w)=1$ and $d=\prod_{j=1}^{t}p_j^{a_j}$, p_j primes. With n,w,d fixed, let $b_{\alpha_1,\ldots,\alpha_t}=\binom{n\prod_{j=1}^{t}p_j^{\alpha_j}}{w\prod_{j=1}^{t}p_j^{\alpha_j}}$.

Theorem 11. *We have*

$$h_{nd,wd}=\frac{1}{nd}\left(\sum_{0\le i_1,\ldots,i_t\le 1}(-1)^{\sum_{j=1}^{t}i_j}\,b_{a_1-i_1,\ldots,a_t-i_t}\right). \tag{4}$$

Proof. We prove the assertion by induction on $a=\sum_{j=1}^{t}a_j$. If $a=0$, or $a=1$, equation 3 shows that $h_{n,w}=\frac{1}{n}\binom{n}{w}$, respectively, $h_{pn,pw}=\frac{1}{np}\left(\binom{np}{wp}-\binom{n}{w}\right)$, for some prime $d=p$.

Now, we need to show the induction step. We consider two cases: *Case* 1 - all $a_i=1$; *Case* 2 - there exists some i with $a_i\ge 2$.

We take Case 1 first. Let $\bar{d}=\prod_{i=2}^{t}p_i$. Any divisor $k\,|'d$, $k\ne d$, is either $p_1,\bar{k}$, or $\bar{k}p_1$, where

$\bar{k}\,|\,\bar{d}$, $\bar{k}\neq 1$. Using this observation together with 3, we obtain

$$
\begin{aligned}
nd\cdot h_{nd,wd} &= \binom{nd}{wd} - \sum_{\bar{k}|\bar{d},\bar{k}\neq 1} \frac{nd}{\bar{k}} h_{\frac{nd}{\bar{k}},\frac{wd}{\bar{k}}} - \sum_{\bar{k}|\bar{d},\bar{k}\neq 1} \frac{nd}{\bar{k}p_1} h_{\frac{nd}{\bar{k}p_1},\frac{wd}{\bar{k}p_1}} - \frac{nd}{p_1} h_{\frac{nd}{p_1},\frac{wd}{p_1}} \\
&= \binom{nd}{wd} - \sum_{\bar{s}|\bar{d},\,\bar{s}\neq\bar{d}} n\bar{s}p_1 h_{n\bar{s}p_1,w\bar{s}p_1} - \sum_{\bar{s}|\bar{d},\,\bar{s}\neq\bar{d}} n\bar{s}h_{n\bar{s},w\bar{s}} - n\bar{d}h_{n\bar{d},w\bar{d}}
\end{aligned}
\tag{5}
$$

Any divisor $\bar{s}$ of $\bar{d}$ is of the form $\bar{s}=\prod_{i=2}^{t} p_i^{\alpha_i}$, with $0\leq\alpha_i\leq 1$ $(2\leq i\leq t)$. Moreover, using the induction assumption (with $\bar{s}\neq\bar{d}$)

$$
\begin{aligned}
n\bar{s}p_1\cdot h_{n\bar{s}p_1,w\bar{s}p_1} &= \sum_{0\leq i_1,i_2,\ldots\leq 1} (-1)^{\sum_{j=1}^{t} i_j} b_{1-i_1,\alpha_2-i_2,\ldots} \\
&= \sum_{0\leq i_2,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{1,\alpha_2-i_2,\ldots} - \sum_{0\leq i_2,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{0,\alpha_2-i_2,\ldots} \\
n\bar{s}\cdot h_{n\bar{s},w\bar{s}} &= \sum_{0\leq i_2,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{0,\alpha_2-i_2,\ldots} \\
n\bar{d}\cdot h_{n\bar{d},w\bar{d}} &= \sum_{0\leq i_2,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{0,a_2-i_2,\ldots}
\end{aligned}
$$

which implies $n\bar{s}p_1\cdot h_{n\bar{s}p_1,w\bar{s}p_1} + n\bar{s}\cdot h_{n\bar{s},w\bar{s}} = \sum_{0\leq i_2,\ldots\leq 1}(-1)^{\sum_{j=2}^{t} i_j} b_{1,\alpha_2-i_2,\ldots}$.

Therefore, we get

$$
\begin{aligned}
nd\cdot h_{nd,wd} = \binom{nd}{wd} &- \sum_{\substack{0\leq\alpha_2,\ldots\leq 1\\ not\ \ all\ \ 1}} \sum_{0\leq i_2,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{1,\alpha_2-i_2,\ldots} \\
&- \sum_{0\leq i_2,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{0,a_2-i_2,\ldots} = b_{1,1,\ldots,1} \\
&- \sum_{0\leq\alpha_2,\ldots\leq 1} \sum_{0\leq i_2,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{1,\alpha_2-i_2,\ldots} + \sum_{0\leq i_2,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{1,a_2-i_2,\ldots} \\
&- \sum_{0\leq i_2,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{0,a_2-i_2,\ldots} = \sum_{0\leq i_1,\ldots\leq 1} (-1)^{\sum_{j=2}^{t} i_j} b_{a_1-i_1,a_2-i_2,\ldots}
\end{aligned}
\tag{6}
$$

since any term in the first sum is cancelled by another: we have a pattern similar to that of the inclusion-exclusion principle (it is even more apparent what happens in the next argument).

The computations are similar in Case 2. Without loss of generality we may assume that $a_1\geq 2$. Let $\bar{d}=\dfrac{d}{p_1^{a_1}}$. Note that as special cases,

$$
h_{np^r,wp^r} = \frac{1}{np^r}\left(\binom{np^r}{wp^r} - \binom{np^{r-1}}{wp^{r-1}}\right) \ \ (\text{for } t=1),
$$

and

$$
h_{np^rq^s,wp^rq^s} = \frac{1}{np^rq^s}\left(b_{r,s}-b_{r,s-1}-b_{r-1,s}+b_{r-1,s-1}\right) \ \ (\text{for } t=2).
$$

Now let us present the proof. Any divisor $k\,|'d$ $(k\neq d)$ is of the form $p_1^i\bar{k}$, $i=1,2,\ldots,a_1$, where $\bar{k}\,|\,\bar{d}$, such that if $i=a_1$, then $\bar{k}\neq\bar{d}$. Using 3 and the induction hypothesis, we get $(\sum'$

denotes the sum with the extra condition that if $i = 0$, then $\bar{k} \neq 1$, and if $i = a_1$, then $\bar{k} \neq \bar{d}$),

$$
\begin{aligned}
nd \cdot h_{nd,wd} &= \binom{nd}{wd} - \sum_{i=0}^{a_1} \sum_{\bar{k}|\bar{d}}{}' \frac{nd}{p_1^i \bar{k}} h_{\frac{nd}{p_1^i \bar{k}}, \frac{wd}{p_1^i \bar{k}}} \\
&= \binom{nd}{wd} - \sum_{j=0}^{a_1-1} \sum_{\bar{s}|\bar{d}} n\bar{s}p_1^j h_{np_1^j \bar{s}, wp_1^j \bar{s}} - \sum_{\bar{s}|\bar{d},\, \bar{s}\neq\bar{d}} np_1^{a_1} \bar{s} h_{np_1^{a_1}\bar{s}, wp_1^{a_1}\bar{s}} \\
&= b_{a_1,\ldots,a_t} - \sum_{j=1}^{a_1-1} \left(\sum_{0\le i_2,\ldots\le 1} (-1)^{\sum_{k=2}^t i_k} b_{j,\alpha_2-i_2,\ldots} - \sum_{0\le i_2,\ldots\le 1} (-1)^{\sum_{k=2}^t i_k} b_{j-1,\alpha_2-i_2,\ldots} \right) \\
&\quad - \sum_{0\le i_2,\ldots\le 1} (-1)^{\sum_{j=2}^t i_j} b_{0,\alpha_2-i_2,\ldots} + \sum_{0\le i_2,\ldots\le 1} (-1)^{\sum_{j=2}^t i_j} b_{a_1,\alpha_2-i_2,\ldots} \\
&= \sum_{0\le i_1,\ldots,i_t\le 1} (-1)^{\sum_{j=1}^t i_j} b_{a_1-i_1,\ldots,a_t-i_t}.
\end{aligned}
\tag{7}
$$

This proves Case 2. Hence the proof. □

3 Rotation symmetric functions with cryptographic significance

With the enumeration results for *RotS* Boolean functions in the previous section, the search space is reduced to a large extent and it seems possible to search this space to check whether there exists cryptographically interesting Boolean functions. The results show that the *RotS* Boolean functions are rich in this context. For detailed discussion about these cryptographic properties see [13] and the references therein. Before stating the results we first need to present some definitions.

Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ in V_n and

$$x \cdot \omega = x_1\omega_1 + \ldots + x_n\omega_n.$$

Let $f(x)$ be a Boolean function on n variables. Then the *Walsh transform* of $f(x)$ is a real valued function over V_n that can be defined as

$$W_f(\omega) = \sum_{x\in V_n} (-1)^{f(x)+x\cdot\omega}.$$

Note that $W_f(\omega) = wd(f, l_\omega)$, where l_ω denotes the linear function on n variables given by $l_\omega(x) = \omega \cdot x$.

The following characterization of correlation immune functions has been presented in [6]. A function $f(x_1, \ldots, x_n)$ is m-th order *correlation immune* (CI) if and only if its Walsh transform satisfies $W_f(\omega) = 0$, for $1 \le wt(\omega) \le m$. Note that f is balanced if and only if $W_f(0) = 0$. Balanced m-th order correlation immune functions are called *m-resilient* functions. Thus, a function $f(x_1, \ldots, x_n)$ is m-resilient if and only if its Walsh transform satisfies $W_f(\omega) = 0$, for $0 \le wt(\omega) \le m$.

By an (n, m, d, u) function we denote an n-variable, m-resilient function with degree d and nonlinearity u. By $(n, 0, d, u)$ function we mean a balanced n-variable function with degree d and nonlinearity u. In the above notation a component is replaced by a '$-$', if it is not specified, e.g., $(n, m, -, u)$, if the degree is not specified.

Define $\Delta_f(\alpha) = wd(f(x), f(x \oplus \alpha))$, the autocorrelation value of f with respect to the vector α. Now we define the Propagation Characteristics of a Boolean function [10]. An n-variable function f is said to satisfy $PC(k)$, if $\Delta_f(\alpha) = 0$ for any α such that $1 \leq wt(\alpha) \leq k$. The absolute indicator is $\Delta_f = \max_{\alpha \in V_n, \alpha \neq 0} |\Delta_f(\overline{\alpha})|$.

3.1 Bent Functions

Bent functions are extremely interesting combinatorial objects [12]. Bent functions on n variables (n even) possess the maximum possible nonlinearity and the Walsh spectra contain only the values $\pm 2^{\frac{n}{2}}$. Further these functions are of algebraic degree at most $\frac{n}{2}$ for $n > 2$.

We now consider the *RotS* bent functions. Consider that there exists a *RotS* bent function f on n variables with $f(0,0,\ldots,0) = 0$ and the ANF of the function is free from the terms $x_1 + \ldots + x_n$. In that case, $1+f, x_1+\ldots+x_n+f$ and $1+x_1+\ldots+x_n+f$ are also *RotS* bent functions. Thus if we count the *RotS* bent functions with $f(0,0,\ldots,0) = 0$ and free from the terms $x_1 + \ldots + x_n$, then multiplying that by 4 we get the total count.

We know that $g_4 = 6$ and $g_6 = 14$. Thus we can easily go for exhaustive search. For 4 variables, there are 8 such functions, and they are represented by the SANF x_1x_3 and $x_1x_2 + x_1x_3$.

For 6 variables, there are 48 *RotS* bent functions, represented by the following 12 functions in SANF :

$$\begin{array}{cc}
x_1x_4, & x_1x_2x_3 + x_1x_4 + x_1x_3x_5, \\
x_1x_3 + x_1x_4 + x_1x_3x_4, & x_1x_3 + x_1x_4 + x_1x_2x_4, \\
x_1x_3 + x_1x_2x_3 + x_1x_4 + x_1x_3x_4 + x_1x_3x_5, & x_1x_3 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_5, \\
x_1x_2 + x_1x_4 + x_1x_3x_4, & x_1x_2 + x_1x_4 + x_1x_2x_4, \\
x_1x_2 + x_1x_2x_3 + x_1x_4 + x_1x_3x_4 + x_1x_3x_5, & x_1x_2 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_5, \\
x_1x_2 + x_1x_3 + x_1x_4, & x_1x_2 + x_1x_3 + x_1x_2x_3 + x_1x_4 + x_1x_3x_5.
\end{array}$$

We also have that $g_8 = 36$. Thus the search over this space needs checking 2^{36} options, which is computationally not very easy. We reduce this space further using the results of Theorem 9 and Corollary 10. First of all we can always assign 0 value corresponding to $g_{8,0}$ many group which forces $f(0,0,\ldots,0) = 0$ and $g_{8,1}$ many group which forces that the ANF is free from the terms $x_1 + \ldots + x_n$. We find the count of such bent functions and then multiply by 4 to get the total count. Further we know that bent functions are of algebraic degree at most $\frac{n}{2}$ for $n > 2$. Thus we can easily discard $g_{8,5} + g_{8,6} + g_{8,7} + g_{8,8}$ many groups as all the monomials containing more than 4 variables will not exist. So the number of groups where we have to assign 0 or 1 values is $g_{8,2} + g_{8,3} + g_{8,4} = 21$ only. Thus we need to search a space of 2^{21} *RotS* functions on 8-variables to get the complete list of *RotS* bent functions on 8 variables. It took 6 hours on a Pentium 1.6 GHz computer with 256 MB RAM using Linux 7.2 operating system. The program has been written in C. We found that there are $4 \cdot 3776$ *RotS* bent functions on 8 variables and the following 8 are homogeneous, expressed in SANF :

$$x_1x_5;\ x_1x_4 + x_1x_5;\ x_1x_3 + x_1x_5;\ x_1x_3 + x_1x_4 + x_1x_5;\ x_1x_2 + x_1x_5;$$
$$x_1x_2 + x_1x_4 + x_1x_5;\ x_1x_2 + x_1x_3 + x_1x_5;\ x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5.$$

We could not exhaustively search beyond 8 variable functions. This is because, for 10 variables, $g_{10} = 108$ and we need to consider functions up to degree 5 and hence $g_{10,2}+g_{10,3}+g_{10,4}+g_{10,5} = 65$ groups for searching bent functions, which needs checking of 2^{65} functions. Homogeneous bent functions are of interest in literature [2, 3, 11]. Though we could not search the complete space of *RotS* bent functions on 10 variables, we could search the homogeneous ones. The SANF of degree 2 homogeneous 10-variable *RotS* bent functions are: x_1x_6, $x_1x_5+x_1x_6$, $x_1x_4+x_1x_6$, $x_1x_3+x_1x_6$,

$x_1x_3 + x_1x_4 + x_1x_6$, $x_1x_3 + x_1x_4 + x_1x_5 + x_1x_6$, $x_1x_2 + x_1x_6$, $x_1x_2 + x_1x_5 + x_1x_6$, $x_1x_2 + x_1x_4 + x_1x_5 + x_1x_6$, $x_1x_2 + x_1x_3 + x_1x_5 + x_1x_6$, $x_1x_2 + x_1x_3 + x_1x_4 + x_1x_6$, $x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_1x_6$.

Note that $g_{10,3} = 12, g_{10,4} = 22$, and $g_{10,5} = 26$. Thus it is possible to search for 10-variable homogeneous *RotS* bent functions with degree 3, 4, and 5. Unfortunately we could not find any evidence of homogeneous bent functions there. Thus we make the following conjecture.

Conjecture 12. *There are no homogeneous RotS bent functions of degree* > 2.

Somewhat related to our conjecture, Xia *et. al.* [16] showed that there are no homogeneous bent functions of degree n in $2n$ variables, for $n > 3$.

3.2 Resiliency and Propagation Characteristics

For an (n, m, d, u) function, $m + d \leq n - 1$ [14] and $u \leq 2^{n-1} - 2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor}$ [1]. From cryptographic point of view, it is important to find functions attaining these bounds. Further it is important to find functions with $PC(k)$, where k is high. Low value of Δ_f is also essential. These functions have important applications in S-boxes [10]. So far, for odd $n < 15$, the lowest possible Δ_f value achieved for balanced functions is $2^{\frac{n+1}{2}}$. We found the evidence of such very important examples in the *RotS* Boolean functions class.

Since we find that the space of *RotS* Boolean functions is much smaller than the complete space of Boolean functions, we can successfully search that space for small values of n. In fact, we did the complete search for $n = 5, 6, 7$ and found the following interesting results. We present the functions in SANF and with $f(0, 0, \ldots, 0) = 0$. The properties balancedness, correlation immunity, resiliency, nonlinearity, algebraic degree, Δ_f and propagation characteristics of a function f stay preserved for the function $1 + f$ also. Hence we count the functions with $f(0, 0, \ldots, 0) = 0$ and double the count value to give the exact number of such functions.

3.2.1 5-variable

There are eight $(5, 1, 3, 12)$ functions, $x_1x_2 + x_1x_3 + x_1x_2x_4$, $x_1x_2 + x_1x_3 + x_1x_2x_3$, $x_1 + x_1x_3 + x_1x_2x_4$, $x_1 + x_1x_2 + x_1x_2x_3$ and their complements. Most interestingly, they possess the theoretically best possible $\Delta_f = 8$ value. That is, these functions provide provably best possible parameters in terms of nonlinearity, resiliency, algebraic degree and autocorrelation values. However, there are no $(5, 2, 2, 8)$ *RotS* function.

All the 5-variable functions, with maximum possible nonlinearity 12, that satisfy propagation characteristics are PC(4). There are 12 functions which are $PC(4)$ and of nonlinearity 12. The Δ_f value for all of them is 32. The functions with $f(0) = 0$ are x_1x_3, x_1x_2, $x_1 + x_1x_2 + x_1x_3$ (balanced) and $x_1x_2 + x_1x_3$, $x_1 + x_1x_3$ and $x_1 + x_1x_2$ (unbalanced).

3.2.2 6-variable

There are fifty two $(6, 1, -, 24)$ *RotS* functions. The algebraic degrees of the functions will be revealed from the SANF presented in Table 3. We present the 26 functions with $f(0) = 0$. The others are their complements. The * marked functions satisfy the $PC(1)$ property and the ** marked functions satisfy $PC(2)$ property in Table 3. There are no $(6, 2, 3, 24)$ and $(6, 3, 2, 16)$ *RotS* functions.

There are $2 \cdot 56$ balanced $PC(1)$ functions with nonlinearity 24. Considering $f(0) = 0$, out of the 56 functions, there are 16 functions with algebraic degree 5 and $\Delta_f = 16$. One example is $x_1x_2x_3 + x_1x_4 + x_1x_3x_4 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_2x_3x_4x_5$.

$\Delta_f = 64$
** x_1x_3
* $x_1x_2 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_3x_5 + x_1x_2x_4x_5$
** $x_1x_2 + x_1x_2x_3 + x_1x_3x_5$
* $x_1 + x_1x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_3x_5 + x_1x_2x_4x_5$
** $x_1 + x_1x_3 + x_1x_2x_3 + x_1x_3x_5$
** $x_1 + x_1x_2$
$\Delta_f = 40$
* $x_1x_3 + x_1x_4 + x_1x_3x_4 + x_1x_2x_4x_5$
* $x_1x_3 + x_1x_4 + x_1x_2x_4 + x_1x_2x_4x_5$
* $x_1x_2 + x_1x_2x_3 + x_1x_4 + x_1x_3x_4 + x_1x_3x_5 + x_1x_2x_4x_5$
* $x_1x_2 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_5 + x_1x_2x_4x_5$
* $x_1 + x_1x_3 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_3x_5$
* $x_1 + x_1x_3 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_3x_5$
$x_1 + x_1x_2 + x_1x_2x_3 + x_1x_3x_4 + x_1x_2x_3x_4$
$x_1 + x_1x_2 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_3x_4$
$\Delta_f = 32$
$x_1x_2 + x_1x_3 + x_1x_3x_4$
$x_1x_2 + x_1x_3 + x_1x_2x_4$
$x_1x_2 + x_1x_3 + x_1x_2x_3 + x_1x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_4x_5$
$x_1x_2 + x_1x_3 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_2x_4x_5$
$x_1 + x_1x_3x_4$
$x_1 + x_1x_2x_4$
$x_1 + x_1x_2x_3 + x_1x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_4x_5$
$x_1 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_2x_4x_5$
$\Delta_f = 24$
$x_1x_2 + x_1x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_4x_5$
$x_1x_2 + x_1x_3 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4$
$x_1 + x_1x_4 + x_1x_2x_4x_5$
$x_1 + x_1x_2x_3 + x_1x_2x_3x_4$

Table 3: The $(6, 1, -, 24)$ *RotS* functions

.

There are $2 \cdot 6$ balanced $PC(2)$ functions with nonlinearity 24. Out of the 6 functions with $f(0) = 0$, there are two functions with algebraic degree 5 and $\Delta_f = 40$, and one of them is $x_1x_2x_3 + x_1x_4 + x_1x_2x_3x_4 + x_1x_3x_5 + x_1x_2x_4x_5 + x_1x_2x_3x_4x_5$ and $x_1x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_4x_5 + x_1x_2x_3x_4x_5$. The other three are of $\Delta_f = 64$.

There are $2 \cdot 16$ unbalanced $PC(2)$ functions with nonlinearity as high as 26. The functions are only 2 away from balancedness, i.e., they are of weight either 30 or 34 (weight of a 6-variable balanced function is 32). Now we consider the 16 functions with $f(0) = 0$. Out of these, 8 have degree 4 and $\Delta_f = 16$, (one example is $x_1x_2 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_3x_5 + x_1x_2x_4x_5$) and 8 have degree 5 and $\Delta_f = 24$, (one example is $x_1x_2 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_3x_4x_5$).

There are $2 \cdot 104$ unbalanced $PC(1)$ functions with nonlinearity 26. Now we consider the 104 functions with $f(0) = 0$. Out of these, 16 have degree 5 and $\Delta_f = 8$. Moreover, four of these are only 2 away from balancedness (one example $x_1x_4 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_3x_4x_5$).

3.2.3 7-variable

There are $2 \cdot 856$ number of $(7, 1, -, 56)$ functions (856 functions with $f(0) = 0$ and their complements). Now we only consider the count of the functions with $f(0) = 0$. There are 42 number of $(7, 1, 5, 56)$ functions with $\Delta_f = 16$. One example is the function $x_1x_3 + x_1x_4 + x_1x_3x_4 + x_1x_2x_4x_5 + x_1x_2x_4x_6 + x_1x_2x_3x_4x_6 + x_1x_2x_3x_5x_6$.

There are 240 number of $(7, 1, 4, 56)$ functions with $\Delta_f = 16$ which also possess the $PC(1)$ property. One example is the function $x_1x_2x_3 + x_1x_4 + x_1x_2x_3x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$. Deterministic construction of these functions are combinatorially challenging and still not known.

Construction of 7-variable, 2-resilient functions with nonlinearity 56 has been considered as one of the extremely hard combinatorial problem. So far there is no existing deterministic construction method to construct these functions. These functions were found by search methods earlier [4, 8]. Running a computer program, we obtained that there are $2 \cdot 36$ number of $(7, 2, 4, 56)$ functions in the *RotS* class. They are listed in Table 4. We mention that all of these functions have $\Delta_f = 16$,

$x_1x_3 + x_1x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5$
$x_1x_3 + x_1x_4 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5$
$x_1x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_6$
$x_1x_2 + x_1x_2x_3 + x_1x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_6$
$x_1x_2 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1x_2 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1x_2 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_2x_4x_6$
$x_1x_2 + x_1x_3 + x_1x_3x_4 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_2x_4x_6$
$x_1x_2 + x_1x_3 + x_1x_2x_4 + x_1x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1x_2 + x_1x_3 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5$
$x_1x_2 + x_1x_3 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5$
$x_1 + x_1x_4 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5$
$x_1 + x_1x_4 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5$
$x_1 + x_1x_2x_3 + x_1x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_2x_3 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_3 + x_1x_2x_3x_4 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_3 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_3 + x_1x_3x_4 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_3 + x_1x_2x_4 + x_1x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_3 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_3 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_3 + x_1x_2x_3 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5$
$x_1 + x_1x_3 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5$
$x_1 + x_1x_2 + x_1x_2x_3x_4 + x_1x_2x_4x_5 + x_1x_3x_4x_5$
$x_1 + x_1x_2 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5$
$x_1 + x_1x_2 + x_1x_2x_3 + x_1x_3x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_2 + x_1x_2x_3 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_2 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_2 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_3x_4x_5 + x_1x_2x_4x_6$
$x_1 + x_1x_2 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5$
$x_1 + x_1x_2 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_3x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5$

Table 4: The $(7, 2, 4, 56)$ *RotS* functions.

which is better than the value 24 presented in [4]. In fact, the $(7, 2, 4, 56)$ function with $\Delta_f = 16$ provides best possible parameters for a 7-variable Boolean function.

4 Conclusion

In this paper we investigated rotation symmetric Boolean functions. We provide complete enumeration results for these functions including the number of such functions with specific degree. Our results show that the search space of rotation symmetric functions is much smaller compared to the complete space of Boolean functions and so we were able to do some experiments on this class of functions. We studied the rotation symmetric bent functions completely up to 8 variables. Further, we observed that up to 10 variables, there is no homogeneous rotation symmetric bent function of degree > 2. It is an important open question to settle the count of rotation symmetric bent functions. We have also checked the cryptographic properties of rotation symmetric functions up to 7 variables. Getting theoretical constructions of these functions instead of search is an interesting research problem. Moreover, any theoretical advancement in this direction can be used to find cryptographically significant functions on higher number of variables.

References

[1] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation immune functions. In *Sequences and Their Applications - SETA 2001*, Discrete Mathematics and Theoretical Computer Science, pages 131–144. Springer Verlag, 2001.

[2] C. Charnes, M. Rötteler, and T. Beth. On Homogeneous Bent Functions. In *Proceedings of Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-14)*, pages 249-259, number 2227 of LNCS, Springer-Verlag, 2001.

[3] C. Charnes, M. Rötteler, and T Beth. Homogeneous Bent Functions, Invariants, and Designs. *Designs, Codes, and Cryptography* (special issue dedicated to Ron Mullin), pages 139-154, vol 26, no 1-3, 2002.

[4] J. Clark, J. Jacob, S. Stepney, S. Maitra and W. Millan. Evolving Boolean Functions Satisfying Multiple Criteria. Accepted in *INDOCRYPT 2002*, to be published in Lecture Notes in Computer Science, Springer Verlag.

[5] T. W. Cusick and P. Stănică. Fast Evaluation, Weights and Nonlinearity of Rotation-Symmetric Functions. *Discrete Mathematics*, pages 289-301, vol 258, no 1-3, 2002.

[6] X. Guo-Zhen and J. Massey. A spectral characterization of correlation immune combining functions. *IEEE Transactions on Information Theory*, pages 569-571, vol 34, no 3, 1988.

[7] S. Moriai, T. Shimoyama and T. Kaneko. Higher order differential attack using chosen higher order differences. In *Selected Areas in Cryptography - SAC '98*, pages 106-117, LNCS 1556, Springer Verlag, 1999.

[8] E. Pasalic, S. Maitra, T. Johansson and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. In *Workshop on Coding and Cryptography - WCC 2001*, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.

[9] J. Pieprzyk and C. X. Qu. Fast Hashing and Rotation-Symmetric Functions. *Journal of Universal Computer Science*, pages 20-31, vol 5, no 1 (1999).

[10] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, pages 161-173, LNCS, Springer-Verlag 1991.

[11] C. Qu, J. Seberry and J. Pieprzyk. Homogeneous bent functions. *Discrete Applied Mathematics*, pages 133-139, vol 102, no 1-2, May 2000.

[12] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, pages 300-305, vol 20, 1976.

[13] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, pages 485-506, number 1807 in LNCS, Springer Verlag, 2000.

[14] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984.

[15] N. J. A. Sloane. On single-deletion-correcting codes. *Codes and Designs - Ray-Chaudhuri Festschrift*, pages 273-292, (Eds. K. T. Arasu and Á. Seress), 2002.

[16] T. Xia, J. Seberry, J. Pieprzyk, C. Charnes, Homogeneous bent functions of degree n in $2n$ variables do not exist for $n > 3$, *Discrete Mathematics*, (to appear).