# Enumeration of Homogeneous Rotation Symmetric Functions over $GF(p)$

Shaojing Fu, Chao Li, Bing Sun

Department of Mathematics and System Science, Science College of National University of Defence Technology, Changsha, China, 410073
shaojing1984@yahoo.cn

**Abstract.** Rotation symmetric functions have been used as components of different cryptosystems. This class of functions are invariant under circular translation of indices. In this paper, we will do some enumeration on homogeneous rotation symmetric functions over $GF(p)$. And we give a formula to count homogeneous rotation symmetric functions when the greatest common divisor of input variable $n$ and the degree $d$ is a power of a prime, which solves the open problem in [7].
**Key words:** Rotation symmetry; Algebraic degree; Minimal function; Monic monomial

## 1 Introduction

In [1], Pieprzyk and Qu studied some functions, which they called rotation symmetric (RotS), as components in the rounds of a hashing algorithm. This class of functions are invariant under circular translation of indices, and it is clear that this class of functions are very rich in terms of many cryptographic properties such as nonlinearity and correlation immune.

As it is the case with every cryptographic property, one is interested to count the objects satisfying that property. This motivates us to look at Boolean functions satisfying various criteria and try to select 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.

In[2-4], Stanica, Maitra and Clark gave many counting results of RotS Boolean functions. They also investigated the correlation immune property of such functions. Dalai and Maitra studied RotS bent functions in [5]. Maximov, Hell and Maitra got many interesting results on plateaued RotS functions in [6]. Yuan Li extended the concept of RotS from $GF(2)$ to $GF(p)$[7], and he gave a formula to count homogeneous rotation symmetric functions with degree no more than 3. We here work in the direction at enumeration of homogeneous RotS functions over $GF(p)$ and provide better results than the previous work.

The paper is organized as follows. Section 2 provides basic definitions and notations. In Section 3, we do some enumeration on homogeneous RotS functions over $GF(p)$ and solve one of the open problems in [7]. Section 4 concludes this paper.

## 2 Preliminaries

In this paper, $p$ is a prime. Let $GF(p)$ be the finite field of $p$ elements, and $\mathrm{GF}(p)^n$ be the vector space of dimension $n$ over $GF(p)$. An $n$-variable function $f(x_1, x_2, \cdots, x_n)$ can be seen as a multivariate polynomial over $GF(p)$, that is,

$$f(x_1, x_2, \cdots, x_n) = \sum_{k_1, k_2, \cdots, k_n = 0}^{n} a_{k_1, k_2, \cdots, k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

where each coefficient $a_{k_1, k_2, \cdots, k_n}$ is a constant in $GF(p)$. This representation of $f$ is called the algebraic normal form (ANF) of $f$. $k_1 + k_2 + \cdots + k_n$ is defined as the degree of term with nonzero coefficient. The greatest degree of all the terms of $f$ is called the Algebraic degree of $f$, denoted by $\deg(f)$. If the degrees of all the terms of $f$ are equal, then we say $f$ is homogeneous.

$f(x)$ is affine if $f(x) = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n + a_0$, and linear if $f(x) = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$. We will denote by $F_n$ the set of all functions of $n$ variables and by $L_n$ the set of affine ones. We will call a function nonlinear if it is not in $L_n$.

If $x_i \in GF(p)$ for any $1 \leq i \leq n$, and $0 \leq k \leq n-1$. We define

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

Let $x = (x_1, \cdots, x_n) \in GF(p)^n$, then the definition of $\rho_n^k$ on tuples and monomials can be extend as follows:

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

and

$$\rho_n^k(x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}) = (\rho_n^k(x_1))^{k_1} \cdots (\rho_n^k(x_n))^{k_n}.$$

**Definition 1.** *A function $f(x_1, x_2, \cdots, x_n)$ over $GF(p)^n$ is RotS if for each input $x = (x_1, \cdots, x_n) \in GF(p)^n$, $f\left(\rho_n^k(x_1, x_2, \cdots, x_n)\right) = f(x_1, x_2, \cdots, x_n)$ for any $0 \leq k \leq n-1$.*

## 3 Enumeration of Balanced RotS Functions

In this section, we will do some enumeration on homogeneous RotS functions over $GF(p)$. Now we start with some important definitions.

**Definition 2.** *A function $f$: $GF(p)^n \rightarrow GF(p)$ is called minimal function if $f$ has the form*

$$f(x_1, x_2, \cdots, x_n) = \sum_{k=0}^{N-1} \rho_n^k(x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n})$$

*where $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ is a monomial of $f$ and $N = \#\{\rho_n^k(x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}) | 0 \leq k \leq n-1\}$.*

**Definition 3.** *A monic monomial $x_1^{y_1}x_2^{y_2}\cdots x_n^{y_n}$ is analogous to $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$, if there exists a permutation $\pi$ on $n$ elements, such that $(k_1,k_2,\cdots,k_n) = (y_{\pi(1)},y_{\pi(2)},\cdots,y_{\pi(n)})$.*

Let $\Omega(d,p,n)$ be the equation system as follow:

$$\Omega(d,p,n):\begin{cases} y_1+y_2+\cdots+y_n=d \\ 0\le y_n\le\cdots\le y_2\le y_1\le p-1 \\ y_i\in\mathbb{Z}(1\le i\le n)\end{cases}$$

Let $N_\Omega$ be the number of solutions of $\Omega(d,p,n)$, and the solutions be $\{(y_1^{(j)},y_2^{(j)},\cdots,y_n^{(j)})|1\le j\le N_\Omega\}$.

In the rest of this paper, we denoted by $T_{n,d}$ the number of minimal functions with degree $d$, and $NU_{n,d}$ is denoted by the number of $n$-variable homogeneous RotS functions over $GF(p)$ with degree $d$.

**Lemma 1.** *Let $m_i^{(j)}(0\le i\le p-1, 1\le j\le N_\Omega,)$ be the number of times that $i$ appears in $\{y_1^{(j)},y_2^{(j)},\cdots,y_n^{(j)})\}(1\le j\le N_\Omega)$, then the number of monic monomials with degree $d$ is $\sum_{j=1}^{N_\Omega}\frac{n!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}$.*

*Proof.* For a fixed $j$ and the corresponding solution $(y_1^{(j)},y_2^{(j)},\cdots,y_n^{(j)})$, the number of monic monomials analogous to $x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}}$ is

$$\binom{n}{m_0^{(j)}}\binom{n-m_0^{(j)}}{m_1^{(j)}}\cdots\binom{n-\sum_{i=1}^{p-2}m_i^{(j)}}{m_{p-1}^{(j)}}=\frac{n!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{(p-1)}^{(j)}!}$$

so the number of monic monomials with degree $d$ is $\sum_{j=1}^{N_\Omega}\frac{n!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}$.

**Theorem 1.** $NU_{n,d}\ge p^{\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}}-1$.

*Proof.* Note that a homogeneous RotS function $f(x_1,x_2,\cdots,x_n)$ with degree $d$ is a nonzero combination of minimal functions with degree $d$. That is

$$f(x_1,x_2,\cdots,x_n)=\sum_{m=1}^{T_{n,d}}a_m g_m(x_1,x_2,\cdots,x_n)$$

where $a_m\in GF(p)$, $g_m(x_1,x_2,\cdots,x_n)$ are minimal functions with degree $d$.

If a minimal function has the term $x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}}$, then it has all the terms in the set $\{\rho_n^k(x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}})|0\le k\le n-1\}$, It is easy to show that $\#\{\rho_n^k(x_1^{y_1^{(j)}}x_2^{y_2^{(j)}}\cdots x_n^{y_n^{(j)}})|0\le k\le n-1\}\le n$. From Lemma 1 we know the number of monic monomials with degree $d$ is $\sum_{j=1}^{N_\Omega}\frac{n!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}$. So the number of minimal functions $T_{n,d}\ge\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}$. Since the constant 0 function is not counted, we get the result.

Note that if $n$ is a prime and $n \nmid d$, then $\#\{\rho_n^k(x_1^{y_1^{(j)}} x_2^{y_2^{(j)}} \cdots x_n^{y_n^{(j)}})|0 \le k \le n-1\} = n$ for any $1 \le j \le N_\Omega$, so we have the following Corollary.

**Corollary 1.** *If $n$ is a prime and $n \nmid d$, then:*

$$NU_{n,d} = p^{\sum_{j=1}^{N_\Omega} \frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}} - 1.$$

In [7], it is an open problem to count $n$-variable homogeneous rotation symmetric functions with degree $d$ more than 3. In the following theorems, we will solve the problem when $gcd(n,d) = 1$ or $gcd(n,d)$ is a power of a prime.

**Theorem 2.** *If $\gcd(d,n) = 1$, then:*

$$T_{n,d} = \sum_{j=1}^{N_\Omega} \frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}.$$

*Proof.* Let $m_i^{(j)} (0 \le i \le p-1, 1 \le j \le N_\Omega)$ as denoted in lemma 1, then $\#\{\rho_n^k(x_1^{y_1^{(j)}} x_2^{y_2^{(j)}} \cdots x_n^{y_n^{(j)}})|0 \le k \le n-1\} = n$. Otherwise, if $\#\{\rho_n^k(x_1^{y_1^{(j)}} x_2^{y_2^{(j)}} \cdots x_n^{y_n^{(j)}})$ $|0 \le k \le n-1\} = N < n$, then $N \mid n$ and $\frac{n}{N} > 1$,

$$\begin{aligned}
&\rho_n^N(x_1^{y_1^{(j)}} x_2^{y_2^{(j)}} \cdots x_n^{y_n^{(j)}}) = x_1^{y_1^{(j)}} x_2^{y_2^{(j)}} \cdots x_n^{y_n^{(j)}} \\
\Rightarrow\ & x_{N+1}^{y_1^{(j)}} x_{N+2}^{y_2^{(j)}} \cdots x_n^{y_2^{(j)}} x_1^{y_2^{(j)}} \cdots x_N^{y_n^{(j)}} = x_1^{y_1^{(j)}} x_2^{y_2^{(j)}} \cdots x_n^{y_n^{(j)}} \\
\Rightarrow\ & \sum_{j=1}^{N} y_1^{(j)} = \sum_{j=N+1}^{2N} y_1^{(j)} = \cdots = \sum_{j=n-N}^{n} y_1^{(j)}
\end{aligned}$$

It is obviously that $\sum_{j=1}^{N} y_1^{(j)} \neq 1$. Then

$$\begin{aligned}
& y_1 + y_2 + \cdots + y_n = d \\
\Rightarrow\ & d = \frac{n}{N} \cdot \sum_{j=1}^{N} y_1^{(j)} \\
\Rightarrow\ & \frac{n}{N} \mid d \\
\Rightarrow\ & \gcd(d,n) = \frac{n}{N}.
\end{aligned}$$

This contradicts with the fact that $\gcd(d,n) = 1$. There are $\sum_{j=1}^{N_\Omega} \frac{n!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}$ monic monomials with degree $d$, so $T_{n,d} = \sum_{j=1}^{N_\Omega} \frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}$.

**Theorem 3.** *If $\gcd(n,d) = q^r (q\ \ prime,\ r \ge 1)$, then we have:*

$$T_{n,d} = \sum_{j=1}^{N_\Omega} \frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!} + \sum_{i=1}^{r} \frac{q^i - 1}{q^i} T_{\frac{n}{q^i}, \frac{d}{q^i}}.$$

*Proof.* First, we make the observation that $T_{n,d}$ is the sum between the number of minimal functions has $n$ terms(abbr. long minimal functions) and the number of minimal functions has terms less than $n$(abbr. short minimal functions). Obviously, $f(x_1,x_2,\cdots,x_n)=\sum_{k=0}^{N-1}\rho_n^k(x_1^{y_1}x_2^{y_2}\cdots x_n^{y_n})$ has terms less than $n$, if and only if there exists a minimal block $b=[y_1,y_2,\cdots,y_t]$ such that $(y_1,y_2,\cdots,y_n)$ is covered by concatenating $m$ copies of $b$. Then it follows that $m$ divides $n$ and $m$ divides $d$, so $m \mid q^r$. Since $b$ is minimal, then it must be $\#\{\rho_n^k(x_1^{y_1}x_2^{y_2}\cdots x_n^{y_t})|0\le k\le n-1\}=n$. Thus

$$\#short\ minimal\ functions=\sum_{i=1}^{r}T_{\frac{n}{q^i},\frac{d}{q^i}}. \tag{1}$$

Let $L$ be the sets of monic monomials of all the long minimal functions, $S$ be the sets of monic monomials of all the short minimal functions. Recall that the total number of monic monomials with degree $d$ is $\sum_{j=1}^{N_\Omega}\frac{n!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}$. Therefore, $|L|=\sum_{j=1}^{N_\Omega}\frac{n!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}-|S|$. The number of long minimal functions is $\frac{1}{n}|L|$. Then it follows that

$$\#long\ minimal\ functions=\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}-\frac{1}{n}\sum_{i=1}^{r}\frac{n}{q^i}T_{\frac{n}{q^i},\frac{d}{q^i}} \tag{2}$$

Putting together 1 and 2, we obtain the number of minimal functions.

The following corollary is the direct result of theorem 2 and theorem 3.

**Corollary 2.** *If* $\gcd(d,n)=1$*, then*

$$NU_{n,d}=p^{\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}}-1.$$

*If* $\gcd(n,d)=q^r(q\ \ prime,\ r\ge 1)$*, then*

$$NU_{n,d}=p^{\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}+\sum_{i=1}^{r}\frac{q^i-1}{q^i}T_{n/q^i,d/q^i}}-1.$$

*Example 1.* We count the number of homogeneous RotS functions with degree 5 over $GF(p)$ ($p\ge 7$,$n\ge 5$).

First, we solve the equation system $\Omega(5,p,n)$, there are seven solutions: $(5,0,\cdots,0),(4,1,0,\cdots,0),(3,2,0,\cdots,0),(3,1,1,0,\cdots,0),(2,2,1,0,\cdots,0),$ $(2,1,1,1,0,\cdots,0),(1,1,1,1,1,0,\cdots,0)$. Then
(1)if $d\nmid n$, $\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}=\frac{(n-1)!}{(n-1)!}+\frac{(n-1)!}{(n-2)!}+\frac{(n-1)!}{(n-2)!}+\frac{(n-1)!}{2!(n-3)!}+\frac{(n-1)!}{2!(n-3)!}+\frac{(n-1)!}{3!(n-4)!}+\frac{(n-1)!}{5!(n-5)!}=\frac{(n-1)(n-2)(n-3)(n+16)}{5!}+(n^2-n+1)$.Then
$NU_{n,5}=p^{\frac{(n-1)(n-2)(n-3)(n+16)}{5!}+(n^2-n+1)}-1$.
(2)if $d\mid n$, $\sum_{j=1}^{N_\Omega}\frac{(n-1)!}{m_0^{(j)}!m_1^{(j)}!\cdots m_{p-1}^{(j)}!}+\frac{d-1}{d}T_{\frac{n}{d},1}=\frac{(n-1)(n-2)(n-3)(n+16)}{5!}+(n^2-n+\frac{9}{5})$.
Then $NU_{n,5}=p^{\frac{(n-1)(n-2)(n-3)(n+16)}{5!}+(n^2-n+\frac{9}{5})}-1$.

## 4 Conclusion

In this paper, we investigated homogeneous rotation symmetric functions over finite field $GF(p)$. We get a lower bound on the number of homogeneous rotation symmetric functions by finding solutions of an equation system, we show that this bound is tight when $n$ is a prime. And we also give a formula to count homogeneous rotation symmetric functions when the greatest common divisor of the number of input variable and the degree is a power of a prime, which solve the open problem in [7]. Besides, for general $n$, it is still an open problem to count the homogeneous rotation symmetric functions.

## Acknowledgments

The work in this paper is supported by the National Natural Science Foundation of China (NO:60573028) and the open research of National Mobile Communications Research Laboratory, Southeast University(NO:W200825).

## References

1. 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).
2. P. Stanica, S. Maitra, Rotation symmetric Boolean functions-count and cryptographic properties, in: R.C. Bose Centenary Symposium on Discrete Mathematics and Applications, Electronic Notes in Discrete Mathematics, Elsevier, vol. 15, December 2002, pp. 139-145.
3. P. Stanica, S. Maitra, A constructive count of rotation symmetric functions, Information Processing Letters 88 (2003)299-304.
4. P. Stanica, S. Maitra, J. Clark, Results on rotation symmetric bent and correlation immune Boolean functions, in: Fast Software Encryption Workshop(FSE 2004), New Delhi, India, LNCS, vol. 3017, Springer Verlag, 2004, pp. 161-177.
5. D.K. Dalai, S. Maitra, S. Sarkar, Results on rotation symmetric bent functions, in: Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA'06, March 2006, pp. 137-156.
6. A. Maximov, M. Hell, S. Maitra, Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables, in: First Workshop on Boolean Functions: Cryptography and Appl- ications, BFCA 05, LIFAR, University of Rouen, France, March 7-9, 2005, pp. 83-104.
7. Yuan Li, Results on rotation symmetric polynomials over GF(p), Information Sciences Letters 178 (2008) 280-286. (2003), 3066-3071.