SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

June 2017, Vol. 60 068103:1–068103:3
doi: 10.1007/s11432-016-9036-y

# Two classes of rotation symmetric semi-bent functions

Qinglan ZHAO[1,2] & Dong ZHENG[2*]

[1]*School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China;*
[2]*National Engineering Laboratory for Wireless Security,*
*Xi'an University of Post and Telecommunications, Xi'an* 710121*, China*

Received October 21, 2016; accepted January 21, 2017; published online April 25, 2017

**Citation** Zhao Q L, Zheng D. Two classes of rotation symmetric semi-bent functions. Sci China Inf Sci, 2017, 60(6): 068103, doi: 10.1007/s11432-016-9036-y

Boolean functions play critical roles in modern cryptography. Over the past decades, Boolean functions satisfying significant cryptographic properties (such as high nonlinearity and high algebraic immunity) have been studied [1, 2]. Semi-bent Boolean functions are a class of Boolean functions with low Walsh-Hadamard transform values (or high nonlinearity). Besides their applications in cryptography, it has been stated that they have a wide use in code-division multiple-access (CDMA) communication systems [3].

Rotation symmetric (RotS) Boolean functions are invariant under the cyclic shifts of input coordinates [4, 5]. They are of interest since they provide candidates for functions with significant cryptographic properties. For instance, odd-variable functions achieving a higher nonlinearity than the best known bounds have been found (see in [6, 7]). Many researchers have investigated and constructed RotS functions for cryptographic applications [8–10]. The goal of this article is to design two new classes of $n$-variable RotS semi-bent Boolean functions.

Filiol and Fontaine [4] found 5-variable RotS semi-bent functions with degrees 2, 3 and 7-variable RotS semi-bent functions with degrees 2, 3, 4, 5, 6 by computer searching. There was no known theoretical construction of RotS semi-bent functions until 2014. The first class of RotS semi-bent functions with degree 3 was developed by Carlet et al. in [8]. Further study is needed to construct RotS semi-bent functions with degree higher than 3. In this article, we propose two classes of $2m$-variable RotS semi-bent functions which contain functions constructed in [8]. To the best of our knowledge, it is the first time to systematically construct $2m$-variable RotS semi-bent functions with degree ranging from 2 to $m$.

We denote the additions of integers over $\mathbb{R}$ by $+$ and $\sum_i$, and over $\mathbb{F}_2$ by $\oplus$ and $\bigoplus_i$. We denote $\mathbb{F}_2^n$ the $n$-dimension vector space over $\mathbb{F}_2$. An $n$-variable Boolean function $f(x)$, where $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Any $n$-variable Boolean function $f$ can be uniquely represented by its algebraic normal form (ANF):

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} c_u \left( \prod_{i=0}^{n-1} x_i^{u_i} \right), \quad c_u \in \mathbb{F}_2. \tag{1}$$

The number of variables in the highest order product term with nonzero coefficient is the algebraic degree of $f(x)$, denoted by $\deg(f)$. The Hamming weight of an $n$-variable Boolean function $f$ is defined to be $wt(f) = |\{x \mid f(x) = 1, x \in \mathbb{F}_2^n\}|$. If

* Corresponding author (email: zhengdong_xupt@sina.com)
The authors declare that they have no conflict of interest.

 

$wt(f) = 2^{n-1}$, we call $f$ is balanced. The Walsh-Hadamard transform of $f(x)$ is an integer valued function over $\mathbb{F}_2^n$ which is defined as

$$W_f(\omega) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus x\cdot\omega}, \tag{2}$$

where $\omega = (\omega_0, \omega_1, \ldots, \omega_{n-1}) \in \mathbb{F}_2^n$ and $x \cdot \omega = x_0\omega_0 \oplus x_1\omega_1 \oplus \ldots \oplus x_{n-1}\omega_{n-1}$. A Boolean function $f$ with $n$ variables is called semi-bent if its Walsh-Hadamard transform satisfies $W_f(\omega) = 0$ or $\pm 2^{\lceil \frac{n+1}{2} \rceil}$, for all $\omega \in \mathbb{F}_2^n$.

We define the left $k$-cyclic shift operator $\rho_n^k$ on $x_i$ as $\rho_n^k(x_i) = x_{(i+k)(\mathrm{mod}\ n)}$ and on vector $x = (x_0, x_1, \ldots, x_{n-1})$ as $\rho_n^k(x) = (\rho_n^k(x_0), \rho_n^k(x_1), \ldots, \rho_n^k(x_{n-1}))$ for $0 \leqslant k \leqslant n-1$. We denote $X$ a monomial $x_{i_0}x_{i_1}\cdots x_{i_l}$ with $0 \leqslant i_0 < i_1 < \cdots < i_l \leqslant n-1$. The definition of $\rho_n^k$ can be extended on monomial $X$ as $\rho_n^k(X) = \rho_n^k(x_{i_0})\rho_n^k(x_{i_1})\cdots\rho_n^k(x_{i_l})$ for $0 \leqslant k \leqslant n-1$. The orbit of $X$, denoted by $O_n(X)$, is defined to be $\{\rho_n^k(x_{i_0}x_{i_1}\cdots x_{i_l}),\ \text{for } 0 \leqslant k \leqslant n-1\}$. We use the lexicographically first element as the representative element of $O_n(X)$. As an example, the representative element of the orbit $\{x_0x_1x_2, x_1x_2x_3, x_2x_3x_0, x_3x_0x_1\}$ is $x_0x_1x_2$. All orbits can generate a partition of the set of all monomials with algebraic degree at most $n$, and we use $\Gamma(n)$ to denote the set of representative elements of all these orbits.

A Boolean function $f$ is a rotation symmetric (RotS) Boolean function if $f(\rho_n^k(x_0, x_1, \ldots, x_{n-1})) = f(x_0, x_1, \ldots, x_{n-1})$, $0 \leqslant k \leqslant n-1$, for each input $x \in \mathbb{F}_2^n$. Every $n$-variable RotS Boolean function has the following expression form:

$$f(x) = \bigoplus_{X\in\Gamma(n)} c_X \left( \bigoplus_{k=0}^{|O_n(X)|-1} \rho_n^k(X) \right), \quad c_X \in \mathbb{F}_2. \tag{3}$$

We assume $\widehat{g}(x) = g(x_0 \oplus x_m, x_1 \oplus x_{m+1}, \ldots, x_{m-1} \oplus x_{2m-1})$ with $g(x_0, x_1, \ldots, x_{m-1})$ being a Boolean function in $m$ variables. Obviously, $\widehat{g}$ is a $2m$-variable RotS Boolean function if $g$ is an $m$-variable RotS Boolean function. For instance, if $g$ is a 5-variable Boolean function with the form $g(x_0, x_1, \ldots, x_4) = \bigoplus_{k=0}^{4} \rho_5^k(x_0x_1x_2x_3)$, then $\widehat{g}$ is

$$\begin{aligned}
&\widehat{g}(x)\\
&= g(x_0 \oplus x_5, x_1 \oplus x_6, \ldots, x_4 \oplus x_9)\\
&= \bigoplus_{k=0}^{4} \rho_{10}^k\big[(x_0 \oplus x_5)(x_1 \oplus x_6)(x_2 \oplus x_7)(x_3 \oplus x_8)\big]\\
&\text{(noting that there is } \rho_{10}^k \text{ instead of } \rho_5^k\text{)}\\
&= \bigoplus_{k=0}^{9} \rho_{10}^k\big(x_0x_1x_2x_3 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_8\\
&\quad \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_4x_7\\
&\quad \oplus x_0x_1x_4x_8 \oplus x_0x_2x_4x_6\big).
\end{aligned} \tag{4}$$

**Theorem 1.** Let $g_1(x)$ be an $m$-variable RotS Boolean function and $f_1(x)$ be an $n$-variable RotS Boolean function of the form

$$f_1(x) = \widehat{g_1}(x_0, \ldots, x_{2m-1}) \oplus \bigoplus_{k=0}^{n-1} \rho_n^k(x_0x_{t_0}), \tag{5}$$

where $n = 2m$ with $m = 2q+1$, $q \geqslant 1$ and $1 \leqslant t_0 \leqslant m-1$. Then $f_1(x)$ is a semi-bent function if and only if $\gcd(2t_0, m) = 1$.

**Example 1.** Let $n = 2m = 6r$, $r$ be odd, and $g_1(x)$ be an $m$-variable Boolean function with the form $g_1(x) = \bigoplus_{k=0}^{r-1} \rho_m^k(x_0x_rx_{2r})$. Then

$$\begin{aligned}
f_1(x) &= \widehat{g_1}(x) \oplus \bigoplus_{k=0}^{n-1} \rho_n^k(x_0x_{t_0})\\
&= \bigoplus_{k=0}^{n-1} \rho_n^k(x_0x_rx_{2r}) \oplus \bigoplus_{k=0}^{2r-1} \rho_n^k(x_0x_{2r}x_{4r})\\
&\quad \oplus \bigoplus_{k=0}^{n-1} \rho_n^k(x_0x_{t_0}),
\end{aligned} \tag{6}$$

where $1 \leqslant t_0 \leqslant m-1$, is a RotS semi-bent function if and only if $\gcd(2t_0, m) = 1$. Thus for odd $r$, $f_t$ in [8], which has the same form as $f_1(x)$ given by (6), can be regarded as a special case of our constructed functions in (5).

**Theorem 2.** Let $m \geqslant 4$ be even, and $n = 2m = 2pr$ with $p \geqslant 2$, $r \geqslant 1$. Let $g_2(x)$ be an $m$-variable RotS Boolean function without quadratic monomials and of the form:

$$g_2(x) = \bigoplus_{X=x_0x_{i_1r}\cdots x_{i_lr}\in\Gamma'(m)} \left[ v_X \bigoplus_{k=0}^{|O_m(X)|-1} \rho_m^k(X) \right], \tag{7}$$

where $\Gamma'(m) = \{X \in \Gamma(m) \mid X = x_0x_{i_1r}\cdots x_{i_lr}$, for $0 \leqslant i_1 < \cdots < i_l \leqslant p-1$ such that $i_j \equiv 0 \pmod 2$ with $1 \leqslant j \leqslant l$ if $r$ is odd$\}$, and $v_X \in \mathbb{F}_2$.

Let $f_2(x)$ be an $n$-variable RotS Boolean function of the form

$$\begin{aligned}
f_2(x) =& \widehat{g_2}(x_0, \ldots, x_{2m-1}) \oplus \bigoplus_{t=1}^{m-1} \left[ c_t \bigoplus_{k=0}^{n-1} \rho_n^k(x_0x_t) \right]\\
&\oplus \bigoplus_{k=0}^{n-1} \rho_n^k(x_0x_{t_0}),
\end{aligned} \tag{8}$$

where $c_t = c_{m-t} \in \mathbb{F}_2$ and $1 \leqslant t_0 \leqslant m-1$. Then we have

(1) When $c_{\frac{m}{2}} = 0$, $f_2$ is semi-bent if and only if $\gcd(2t_0, m) = 2$ and $\gcd(t_0, m) = 1$.

(2) When $c_{\frac{m}{2}} = 1$ and $m \equiv 0 \pmod 4$, $f_2$ is semi-bent if and only if $\gcd(2t_0, m) = 2$ and $\gcd(t_0, m) = 1$; when $c_{\frac{m}{2}} = 1$ and $m \equiv 2 \pmod 4$, $f_2$ is semi-bent if and only if $\gcd(2t_0, m) = 2$ and $\gcd(t_0, m) = 2$.

(3) $\deg(f_2) = \deg(g_2)$, if $\deg(g_2) \geqslant 3$.

**Example 2.** Let $n = 2m = 6r$, $r$ be even, and $g_2(x)$ be an $m$-variable Boolean function with the form $g_2(x) = \bigoplus_{k=0}^{r-1} \rho_m^k(x_0 x_r x_{2r})$. Similarly to Example 1 we get a class of cubic RotS semi-bent functions with the form

$$f_2(x) = \widehat{g_2}(x) \oplus \bigoplus_{k=0}^{n-1} \rho_n^k(x_0 x_{t_0}),$$

which implies the semi-bent function $f_t$ in [8] for even $r$ also is a special case of our functions.

**Remark 1.** We can construct balanced RotS semi-bent functions based on Theorem 1 by restricting the value of $g_1(\mathbf{1})$, $g_1(\mathbf{0})$ and $t_0$ (or Theorem 2 by restricting the value of $g_2(\mathbf{1})$, $g_2(\mathbf{0})$, $g_2(0, 1, 0, 1, \ldots, 0, 1)$, $g_2(1, 0, 1, 0, \ldots, 1, 0)$ and $t_0$).

**Acknowledgements** This work was supported by National Natural Science Foundation of China (Grant Nos. 61472472, 61272037, 61402366) and Natural Science Basic Research Plan in Shaanxi Province of China (Grant Nos. 2016JM6033, 2015JQ6262). Qinglan ZHAO is supported by New Star Team of Xi'an University of Posts and Telecommunications.

**Supporting information** The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

## References

1 Zhang F R, Carlet C, Hu Y P, et al. New secondary constructions of bent functions. Appl Algebra Eng Commun Comput, 2016, 27: 413–434
2 Zhang W G, Xiao G Z. Construction of almost optimal resilient Boolean functions via concatenating Maiorana-Mcfarland functions. Sci China Inf Sci, 2011, 54: 909–912
3 Mesnager S. On semi-bent functions and related plateaued functions over the galois field $\mathbb{F}_2^n$. In: Open Problems in Mathematics and Computational Science. Berlin: Springer, 2014. 243–273
4 Filiol E, Fontaine C. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In: Advances in Cryptology—EUROCRYPT'98. Berlin: Springer, 1998. 475–488
5 Pieprzyk J, Qu C X. Rotation-symmetric functions and fast hashing. In: Proceedings of the 3rd Australasian Conference on Information Security and Privacy. London: Springer, 1998. 169–180
6 Kavut S, Maitra S. Patterson—Wiedemann type functions on 21 variables with nonlinearity greater than bent concatenation bound. IEEE Trans Inf Theory, 2016, 62: 2277–2282
7 Kavut S, Maitra S, Yücel M D. Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE Trans Inf Theory, 2007, 53: 1743–1751
8 Carlet C, Gao G P, Liu W F. Results on constructions of rotation symmetric bent and semi-bent functions. In: Sequences and Their Applications-SETA 2014. Berlin: Springer, 2014. 21–33
9 Gao G P, Zhang X Y, Liu W F, et al. Constructions of quadratic and cubic rotation symmetric bent functions. IEEE Trans Inf Theory, 2012, 58: 4908–4913
10 Stănică P, Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties. Discrete Appl Math, 2008, 156: 1567–1580