SCIENCE CHINA
Information Sciences

• LETTER •

July 2016, Vol. 59 079102:1–079102:3
doi: 10.1007/s11432-016-5569-x

New constructions of q-variable 1-resilient rotation symmetric functions over $\mathbb{F}_p$

Jiao DU[1,2,3], Shaojing FU[4], Longjiang QU[1], Chao LI[1*] & Shanqi PANG[2,3]

[1]*College of Science, National University of Defense Technology, Changsha* 410073*, China;*
[2]*School of Mathematics and Information Science, Henan Normal University, Xinxiang* 453007*, China;*
[3]*Henan Engineering Laboratory for Big Data Statistical Analysis and Optimal Control, Henan Normal University, Xinxiang* 453007*, China;*
[4]*College of Computer Science, National University of Defense Technology, Changsha* 410073*, China*

Received October 6, 2015; accepted December 29, 2015; published online May 13, 2016

Citation Du J, Fu S J, Qu L J, et al. New constructions of q-variable 1-resilient rotation symmetric functions over $\mathbb{F}_p$. Sci China Inf Sci, 2016, 59(7): 079102, doi: 10.1007/s11432-016-5569-x

Dear editor,

Motivated by Refs. [1–10], we devote to constructing a class of q-variable 1-resilient rotation symmetric functions (RSFs) over the finite field $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ in this letter. Throughout this letter, let p and q be different odd prime numbers.

Notions and main results. Let $|O|$ represent the cardinality of the set O, and $\mathbb{F}_p^n$ be the n dimensional vector space over $\mathbb{F}_p$. The mapping $f : \mathbb{F}_p^n \to \mathbb{F}_p$ represents a generalized n-variable Boolean function, the set of generalized Boolean functions with n variables over $\mathbb{F}_p^n$ is denoted by $\boldsymbol{B}_{n,p}$. Let $f(x) \in \boldsymbol{B}_{n,p}$, and $f^{-1}(l) = \{x \in \mathbb{F}_p^n \mid f(x) = l, l \in \mathbb{F}_p\}$. Then we say that $f(x)$ is balanced if $|f^{-1}(l)| = p^{n-1}$ holds for any $l \in \mathbb{F}_p$. A set S of vectors can be seen as a matrix whose row vectors are the elements of S, without consideration of the order of these elements. $f^{-1}(l)$ is also called the l-value support table of $f(x)$ [7,8].

Definition 1 ([9,10]). An $w \times n$ matrix $\boldsymbol{C}$ over $\mathbb{F}_p$ is called an orthogonal array of strength d, denoted by $\mathrm{OA}(w, n, p, d)$ for simplicity, if each vector in $\mathbb{F}_p^d$ occurs the same number of times in the submatrix of $\boldsymbol{C}$ composed of arbitrary d columns of $\boldsymbol{C}$. $\{V_0, V_1, \ldots, V_{p-1}\}$ is called a large set of orthogonal arrays of strength d over $\mathbb{F}_p^n$ if V_l is an $\mathrm{OA}(p^{n-1}, n, p, d)$ for each $l \in \{0, 1, \ldots, p-1\}$ and the union of elements in $\{V_0, V_1, \ldots, V_{p-1}\}$ forms the vector space $\mathbb{F}_p^n$.

Definition 2 ([9, 10]). If $f(x) \in \boldsymbol{B}_{n,p}$, then $f(x)$ is called a t-resilient function over $\mathbb{F}_p$ if and only if all the vectors in $f^{-1}(l)$ make up an $\mathrm{OA}(p^{n-1}, n, p, t)$ for each $l \in \mathbb{F}_p$.

Let us consider the action of the cyclic group $\{\rho_n^l | 0 \leqslant l \leqslant n-1\}$ on $\mathbb{F}_p^n$, where $\rho_n^l(x_1, x_2, \ldots, x_n) = (x_{l+1}, x_{l+2}, \ldots, x_n, x_1, \ldots, x_l)$, and $0 \leqslant l \leqslant n-1$. The rotation symmetric orbit of x under the action of ρ_n^l is denoted by $\mathrm{RO}_n(x) = \{\rho_n^l(x) | 0 \leqslant l \leqslant n-1\}$, where $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_p^n$. If n is given, $\mathrm{RO}_n(x)$ can be simplified as RO_x. We call $\mathrm{RO}_n(x)$ a long rotation symmetric orbit if $|\mathrm{RO}_n(x)| = n$, otherwise a short rotation symmetric orbit.

Definition 3 ([2–4]). $f(x) \in \boldsymbol{B}_{n,p}$ is called a RSF if $f(\rho_n^l(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n)$ for any $x \in \mathbb{F}_p^n$ and any l.

From Definitions 1–3, it is obvious that construction of an 1-resilient q-variable rotation symmetric function over $\mathbb{F}_p$ is equivalent to dividing p^q vectors into p groups, i.e., $V_0, V_1, V_2, \ldots, V_{p-1}$,

* Corresponding author (email: lichao_nudt@sina.com)

The authors declare that they have no conflict of interest.

satisfying all the vectors in a rotation symmetric orbit must be in the same group and $\{V_0, V_1, V_2, \ldots, V_{p-1}\}$ is a large set of orthogonal arrays of strength 1 [9,10].

Definition 4 ([1])**.** Let S_n be the symmetric group on the set $\{1, 2, \ldots, n\}$. $f(x_1, x_2, \ldots, x_n)$ is called a symmetric function if for any $\pi \in S_n$, we have $f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) = f(x_1, x_2, \ldots, x_n)$.

By Definition 4, if the symmetric group S_q acts on x for each $x \in \mathbb{F}_p^q$, then it generates an orbit such as $O_x = \{(y_1, y_2, \ldots, y_q) | (y_1, y_2, \ldots, y_q) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(q)})\}$. Let $\overline{x} = (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_q})$ be the representative of O_x, where $\overline{x_1} \leqslant \overline{x_2} \leqslant \cdots \leqslant \overline{x_q}$. Assume that

$$\overline{x} = (\underbrace{0, \ldots, 0}_{i_0}, \underbrace{1, \ldots, 1}_{i_1}, \ldots, \underbrace{p-1, \ldots, p-1}_{i_{p-1}}),$$

where $i_0 + i_1 + \cdots + i_{p-1} = q$, and $0 \leqslant i_l \leqslant q$ for each $l \in \mathbb{F}_p$. It is clear that $|O_x| = C(q, i_0, i_1, \ldots, i_{p-2}, i_{p-1}) = \frac{q!}{i_0! i_1! \cdots i_{p-1}!}$ [1].

Definition 5. Let $x = (x_1, x_2, \ldots, x_q) \in \mathbb{F}_p^q$, x is called an $(i_0, i_1, \ldots, i_{p-1})$-**form** vector if the number of times l appears in the vector x is i_l, where $l \in \mathbb{F}_p$. RO_x is said to be $(i_0, i_1, \ldots, i_{p-1})$-**form** if all the vectors in RO_x are $(i_0, i_1, \ldots, i_{p-1})$-**form**, and denote it as $\mathbf{Form}(\mathrm{RO}_x) = (i_0, i_1, \ldots, i_{p-1})$.

Lemma 1 ([1])**.** The number of n-variable symmetric polynomials over $\mathbb{F}_p$ is $p^{C(n+p-1,n)}$, where $C(n, k) = n!/(k!(n-k)!)$.

By Lemma 1, if $n = q$, then there are $C(p+q-1, q)$ different classes of symmetric orbits in $\mathbb{F}_p^q$. So the total number of the **forms** is $C(p+q-1, q)$.

Lemma 2 ([1,2])**.** Let $h_{n,p}$ be the number of long rotation symmetric orbits over $\mathbb{F}_p^n$. Then $h_{1,p} = p$ and $h_{q^s,p} = (p^{q^s} - p^{q^{s-1}})/q^s$.

Lemma 3. Let $f(x)$ be an n-variable RSF over $\mathbb{F}_p$. If $f^{-1}(l) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_n)$, where $\boldsymbol{c}_i$ is the ith column vector of $f^{-1}(l)$, $1 \leqslant i \leqslant n$ and $l \in \mathbb{F}_p$, then there exists a permutation matrix P such that $\boldsymbol{c}_{i+k(\mathrm{mod}\ n)} = \mathrm{P}^k \boldsymbol{c}_i$, where the subscripts are computed modulo n with only exception that when $i + k \equiv 0 \pmod{n}$ by n instead of 0.

Lemma 3 can be proved by the similar method in [7]. By Lemma 3, we have the following result:

Lemma 4. Suppose that the notions are defined as Lemma 3. Then $f(x)$ is 1-resilient if and only if $\boldsymbol{c}_1$ is an $\mathrm{OA}(p^{n-1}, 1, p, 1)$ for each $f^{-1}(l)$.

Let $\boldsymbol{e}_{n,i} = (\underbrace{i, i, \ldots, i}_{n})$ be the row vector of n consecutive i, and $\boldsymbol{e}_{n,i}^{\mathrm{T}}$ be the transpose of $\boldsymbol{e}_{n,i}$.

Note that all the long rotation symmetric orbits are divided into $N = C(p+q-1, q) - p$ different classes according to the **forms** of the rotation symmetric orbits. We arrange those sets by a certain order, say $\Omega_1, \Omega_2, \ldots, \Omega_N$. If the **form** of the rotation symmetric orbits in Ω_j is $(i_{j,0}, i_{j,1}, \ldots, i_{j,p-1})$, then the number of rotation symmetric orbits in Ω_j $(1 \leqslant j \leqslant N)$ is $\frac{(q-1)!}{i_{j,0}! i_{j,1}! \cdots i_{j,p-1}!}$. Let all the **forms** of long rotation symmetric orbits be the rows of the following matrix in a certain order, i.e.,

$$\boldsymbol{I} = \begin{pmatrix} i_{1,0} & i_{1,1} & \cdots & i_{1,p-1} \\ i_{2,0} & i_{2,1} & \cdots & i_{2,p-1} \\ \vdots & \vdots & \cdots & \vdots \\ i_{N,0} & i_{N,1} & \cdots & i_{N,p-1} \end{pmatrix} = \begin{pmatrix} \mathrm{I}_1 \\ \mathrm{I}_2 \\ \vdots \\ \mathrm{I}_N \end{pmatrix},$$

where I_u is the uth row of $\boldsymbol{I}$, which is the **form** of the long rotation symmetric orbits in Ω_u. For simplicity and convenience, we denote $\mathrm{RSO}(\mathrm{I}_u)$ as the set composed of all the rotation symmetric orbits whose **form** is I_u, where $1 \leqslant u \leqslant N$.

Considering the action of the cyclic group $\{\rho_p^l | 0 \leqslant l \leqslant p-1\}$ on the set $\boldsymbol{I}$, we have $m = \frac{N}{p}$ different orbits as follows: $\Delta_k = \{\mathrm{I}_{j_k}, \rho_p(\mathrm{I}_{j_k}), \ldots, \rho_p^{p-1}(\mathrm{I}_{j_k})\}$, where $1 \leqslant k \leqslant m$ and $\boldsymbol{I} = \bigcup_{k=1}^{m} \Delta_k$. If $\mathrm{I}_{j_k} = (i_{j_k,0}, i_{j_k,1}, \ldots, i_{j_k,p-1})$, then we have $n_k = |\mathrm{RSO}(\rho_p^l(\mathrm{I}_{j_k}))| = \frac{(q-1)!}{i_{j_k,0}! i_{j_k,1}! \cdots i_{j_k,p-1}!}$, where $0 \leqslant l \leqslant p-1, 1 \leqslant k \leqslant m$. Now, we present the properties of the **forms** are in Δ_k:

Theorem 1. Let the notions be defined as before, $Q_l \in \mathrm{RSO}(\rho_p^l(\mathrm{I}_{j_k}))$ for $0 \leqslant l \leqslant p-1$, where $1 \leqslant k \leqslant m$. Then the following matrix $\boldsymbol{Q}$ is an $\mathrm{OA}(pq, q, p, 1)$:

$$\boldsymbol{Q} = \begin{pmatrix} Q_0 \\ Q_1 \\ \vdots \\ Q_{p-1} \end{pmatrix} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_q).$$

Suppose that r, g are both nonnegative integers such that $\frac{p^{q-1}-1}{q} = p \cdot g + r, 1 \leqslant r \leqslant p-1, g \geqslant 0$. Then we have $w = \frac{r \cdot q + 1}{p} = p^{q-2} - q \cdot g$.

Theorem 2. Let $\boldsymbol{e}_i = (\underbrace{0, 0, \ldots, 0}_{i-1}, 1, \underbrace{0, 0, \ldots, 0}_{p-i})$. If the following equation system

$$\begin{cases} \boldsymbol{e}_{r,1} \boldsymbol{X} = \boldsymbol{e}_{p,w} - \boldsymbol{e}_1, \\ \boldsymbol{X} \boldsymbol{e}_{p,1}^{\mathrm{T}} = \boldsymbol{e}_{r,q}^{\mathrm{T}} \end{cases} \tag{1}$$

has a solution

$$\boldsymbol{X} = \begin{pmatrix} x_{1,0} & x_{1,1} & \cdots & x_{1,p-1} \\ x_{2,0} & x_{2,1} & \cdots & x_{2,p-1} \\ \vdots & \vdots & \cdots & \vdots \\ x_{r,0} & x_{r,1} & \cdots & x_{r,p-1} \end{pmatrix} = \begin{pmatrix} \mathsf{x}_1 \\ \mathsf{x}_2 \\ \vdots \\ \mathsf{x}_r \end{pmatrix}$$

satisfying the following conditions: (a) $x_{u,v} \in \{0, 1, \ldots, q-1\}, 1 \leqslant u \leqslant r, 0 \leqslant v \leqslant p-1$; (b) x_i is the ith row vector of $\boldsymbol{X}$ such that

$$\bigcup_{i=1}^{l_1}\{\mathsf{x}_i\}\subseteq\Delta_{k_1},\ \bigcup_{i=l_1+1}^{l_1+l_2}\{\mathsf{x}_i\}\subseteq\Delta_{k_2},\ \bigcup_{i=l_1+l_2+1}^{l_1+l_2+l_3}\{\mathsf{x}_i\}\subseteq\Delta_{k_3},\ldots,\ \bigcup_{i=r-l_t+1}^{r}\{\mathsf{x}_i\}\subseteq\Delta_{k_t},$$

where $1\leqslant t\leqslant r<p$, $1\leqslant l_j\leqslant n_{k_j}$, $1\leqslant j\leqslant t$, $1\leqslant k_1,k_2,\ldots,k_t\leqslant m$, and $l_1+l_2+\cdots+l_t=r$, then there exist p different OAs$(rq+1,q,p,1)$, denoted as $B_0,B_1,\ldots,B_{p-1}$, such that $\boldsymbol{e}_{q,i}\in B_i$, $B_i\bigcap B_j=\emptyset$ for $\{i,j\}\subseteq\mathbb{F}_p$, and each B_i contains r number of long rotation symmetric orbits.

Suppose that $1\leqslant s\leqslant\lambda$, $y_{i,j}$ are nonnegative integers for $1\leqslant i\leqslant m=\frac{N}{p},0\leqslant j\leqslant p-1$, and the symbols are defined before. If the equation system

$$\Theta_r:\begin{cases}\boldsymbol{e}_{p,1}\boldsymbol{Y}=(n_1,n_2,\ldots,n_{k_1-1},n_{k_1}-l_1,n_{k_1+1},\ldots,n_{k_2-1},n_{k_2}-l_2,n_{k_2+1},\ldots,n_{k_t-1},\\ \qquad n_{k_t}-l_t,n_{k_t+1},\ldots,n_m),\\ \boldsymbol{Y}\boldsymbol{e}_{m,1}^{\mathrm{T}}=\boldsymbol{e}_{p,g}^{\mathrm{T}},\ \text{where } g=\frac{p^{q-1}-1-qr}{pq},\ \text{ and } 1\leqslant r\leqslant p-1,g\geqslant 0\end{cases}$$

has λ different solutions as follows:

$$\boldsymbol{Y}^s=\begin{pmatrix}y_{1,0}^s & y_{2,0}^s & \cdots & y_{m,0}^s\\ y_{1,1}^s & y_{2,1}^s & \cdots & y_{m,1}^s\\ \vdots & \vdots & \cdots & \vdots\\ y_{1,p-1}^s & y_{2,p-1}^s & \cdots & y_{m,p-1}^s\end{pmatrix},$$

$\boldsymbol{Y}^{s_1}$ is different from $\boldsymbol{Y}^{s_2}$ means that there does not exist any $p\times p$ permutation matrix $\boldsymbol{T}$ such that $\boldsymbol{Y}^{s_1}=\boldsymbol{T}\boldsymbol{Y}^{s_2}$, where $1\leqslant s,s_1,s_2\leqslant\lambda$.

Theorem 3. Let the notions and symbols be defined as before. We assume that $\boldsymbol{X}$ is a solution of the equation system (1) such that $r=t$, $l_1=l_2=\cdots=l_t=1$, and $J=\{k_1,k_2,\ldots,k_t\}\subseteq\{1,2,\ldots,m\}$. If the equation system Θ_r with respect to $\boldsymbol{X}$ has λ different solutions as above $\boldsymbol{Y}^s$, where $1\leqslant s\leqslant\lambda$, then the number of q-variable 1-resilient RSFs over $\mathbb{F}_p$ constructed by the method proposed above is $\boldsymbol{N}=\sum_{s=1}^{\lambda}p!E_sF_s$, where $E_s=\prod_{j\in J}\frac{(n_{k_j}!)^p}{\prod_{l=0}^{p-1}(y_{j,l}^s!)^{p-1}(y_{j,l}^s+1)!}$ and $F_s=(\prod_{k=1,k\notin J}^{m}\frac{n_k!}{y_{k,0}^s!\cdot y_{k,1}^s!\cdots y_{k,p-1}^s!})^p$.

Corollary 1. Let the notions be defined as before, $r=1$, $(w-1,w,w,\ldots,w)\in\Delta_{k_1}$, where $w=\frac{r\cdot q+1}{p}=\frac{q+1}{p}$. If Θ_r has the following μ different solutions

$$\boldsymbol{Y}^{\nu}=\begin{pmatrix}y_{1,0}^{\nu} & y_{2,0}^{\nu} & \cdots & y_{m,0}^{\nu}\\ y_{1,1}^{\nu} & y_{2,1}^{\nu} & \cdots & y_{m,1}^{\nu}\\ \vdots & \vdots & \cdots & \vdots\\ y_{1,p-1}^{\nu} & y_{2,p-1}^{\nu} & \cdots & y_{m,p-1}^{\nu}\end{pmatrix},$$

where $1\leqslant\nu\leqslant\mu$, then the number of q-variable 1-resilient RSFs over $\mathbb{F}_p$ constructed by the method proposed above is

$$\boldsymbol{N}=\sum_{\nu=1}^{\mu}\frac{p!}{\prod_{j=0}^{p-1}(y_{k_1,j}^{\nu}+1)}\left[\prod_{l=1}^{m}\frac{n_l!}{y_{l,0}^{\nu}!y_{l,1}^{\nu}!\cdots y_{l,p-1}^{\nu}!}\right]^p.$$

In order to demonstrate the method proposed in Theorem 3, we give a simple example in Supplementary File.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61272484, 61572026, U1404601, 11571094) and Program for Innovative Research Team (in Science and Technology) in University of Henan Province (Grant No. 14IRTSTHN023).

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 Cusick T W, Li Y, Stânicâ P. Balanced symmetric functions over $GF(p)$. IEEE Trans Inf Theory, 2008, 54: 1304–1307
2 Li Y. Results on rotation symmetric polynomials over $GF(p)$. Inf Sci, 2008, 178: 280–286
3 Fu S J, Qu L J, Li C, et al. Balanced rotation symmetric Boolean functions with maximum algebraic immunity. IET Inform Secur, 2011, 5: 93–99
4 Fu S J, Li C, Matsuura K, et al. Enumeration of balanced symmetric functions over $GF(p)$. Inf Process Lett, 2010, 110: 544–548
5 Ke P H, Huang L L, Zhang S Y. Improved lower bound on the number of balanced symmetric functions over $GF(p)$. Inf Sci, 2009, 179: 682–687
6 Zhang W G, Jiang F Q, Tang D. Construction of highly nonlinear resilient Boolean functions satisfying strict avalanche criterion. Sci China Inf Sci, 2014, 57: 049101
7 Du J, Wen Q Y, Zhang J, et al. Constructions of resilient rotation symmetric Boolean functions on given number of variables. IET Inform Secur, 2014, 8: 265–272
8 Du J, Pang S Q, Wen Q Y, et al. Construction and count of 1-resilient rotation symmetric Boolean functions on p^r variables. Chin J Electron, 2014, 23: 816–820
9 Stinson D R. Resilient functions and large sets of orthogonal arrays. Congressus Numer, 1993, 92: 105–110
10 Gopalakrishnan K, Stinson D R. Three characterizations of non-binary correlation-immune and resilient functions. Des Codes Cryptogr, 1995, 5: 241–251