SCIENCE CHINA
Information Sciences

• **Supplementary File** •

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

DU Jiao[1,2,3], FU ShaoJing[4], QU LongJiang[1], LI Chao[1*] & PANG ShanQi[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*

Appendix A Introduction

Filiol and Fontaine introduced that idempotents are polynomials over finite field of characteristic 2 such that $f(z) = f(z^2)$ for each element z in this finite field [1,2,3], and rotation symmetric Boolean functions(RSBFs) were proposed by Pieprzyk and Qu in [2]. In fact, as pointed out in [3], RSBFs can be obtained from idempotents through proper choices of the normal basis in the corresponding finite field. Hereafter, RSBFs are extensively applied as they are very fast to implement [2]. For examples, firstly, Pieprzyk and Qu studied RSBFs as components in the round of a hashing algorithm and in the implementation of MD4, MD5 or HAVAL [2]. Secondly, RSBFs are used to design Substitution Boxes in block ciphers as well [4,5]. Rotation symmetric bent and semibent Boolean functions are studied by a series of papers [3,5-8]. For the detailed descriptions of the applications of RSBFs in coding theory and cryptography, please refer to the papers [1-4,9-12].

Recently, the RSBFs have received a lot of attention in terms of their cryptographic properties [3,9-16]. It has been experimentally demonstrated that there are a lot of RSBFs with many good cryptographic properties, such as balancedness, high nonlinearity, correlation immunity, high algebraic degree and maximum algebraic immunity [9-16]. Especially, 8-variable, algebraic degree 6, nonlinearity 116, 1-resilient rotation symmetric Boolean functions with maximum absolute value in the autocorrelation spectra 32 was given for the first time in [3]. Based on the computer program, many 1-resilient RSBFs with other good cryptographic properties had been found [10,11], and RSBFs had become the main objects on searching for Boolean functions with good cryptographic properties [8-12]. These results inspire us to find Boolean functions with good cryptographic properties from the class of 1-resilient RSBFs. Constructions and enumerations of correlation immune and resilient rotation symmetric Boolean functions were proposed by a series of papers [3,10,11,17-22].

It is natural and interesting to extend different cryptographic notions and ideas from the binary finite field $\mathbb{F}_2$ to $\mathbb{F}_p$ or $\mathbb{F}_p^n$ [23], where p is an odd prime number. The results in finite fields with odd characteristic may also facilitate the research in even characteristic. Bent functions , perfect nonlinear functions and almost perfect nonlinear functions are good examples. In recent years, rotation symmetric functions over $\mathbb{F}_p$(RSFs for simplicity) have received more attention [23-28]. Symmetric functions are a special class of RSFs. Li and Cusick studied the linear structures of symmetric functions over $\mathbb{F}_p$ [25]. Additionally, several constructions and enumerations of balanced symmetric functions over $\mathbb{F}_p$ were proposed in Ref. [23,24,26]. The authors also presented a lower bound on the number of balanced symmetric functions over $\mathbb{F}_p$ and an equivalent characterization were proposed [26]. The enumeration of RSFs over $\mathbb{F}_p$ was also investigated in Ref. [27,28]. New results on the resilient functions were also given in [29-31] recently. Throughout this paper, we assume that p and q are different odd prime numbers. Motivated by Ref. [23,24,27], we devote to constructing a class of q-variable 1-resilient RSFs over $\mathbb{F}_p$ in this study.

The rest of this Supplementary file is organized as follows. In Appendix B, proof of the main results and some remarks are presented. An illustrative example is demonstrated in Appendix C, and a class of 5-variable 1-resilient RSFs over $\mathbb{F}_3$ were presented. Appendix D concludes the letter.

[*] Corresponding author (email: lichao_nudt@sina.com(LI Chao))

Appendix B Proof of the main results and some remarks

From now on, we study the constructions of a class of q-variable 1-resilient rotation symmetric functions over $\mathbb{F}_p$.

Let g_n be the number of such rotation symmetric orbits. Then it follows from Burnside's lemma that there are p^{g_n} n-variable RSFs, where $g_n = \frac{1}{n}\sum\limits_{k|n}\phi(k)\cdot p^{\frac{n}{k}}$, and $\phi(\cdot)$ is the Euler *phi*-function(see [12,24,27]). If $n = q$, then the total number of rotation symmetric orbits is $g_q = \frac{1}{q}\sum\limits_{t|q}\phi(t)p^{\frac{q}{t}} = p\cdot\frac{p^{q-1}-1}{q} + p$. By Lemma 2, the total number of long rotation symmetric orbits is $h_{q,p} = p\cdot\frac{p^{q-1}-1}{q}$.

Since $p^{q-1}-1$ is not a multiple of p, similar as proved in [27], the vectors in the set $\{e_{q,l}|0\leqslant l\leqslant p-1\}$ must take the different value for different l to keep $f(x)$ to be balanced. In other words, each $V_l(0\leqslant l\leqslant p-1)$ contains a short rotation symmetric orbit, and $\frac{p^{q-1}-1}{q}$ long rotation symmetric orbits.

Considering the action of the cyclic group $\{\rho_p^l|0\leqslant l\leqslant p-1\}$ on the set $\mathbf{I}$, we have $m = \frac{N}{p}$ different orbits as follows:

$$\Delta_k = \{\mathrm{I}_{j_k}, \rho_p(\mathrm{I}_{j_k}), \cdots, \rho_p^{p-1}(\mathrm{I}_{j_k})\}, 1\leqslant k\leqslant m \quad \text{and} \quad \mathbf{I} = \bigcup_{k=1}^{m}\Delta_k.$$

If $\mathrm{I}_{j_k} = (i_{j_k,0}, i_{j_k,1}, \cdots, i_{j_k,p-1})$, then we have

$$n_k = |RSO(\rho_p^l(\mathrm{I}_{j_k}))| = \frac{(q-1)!}{i_{j_k,0}!i_{j_k,1}!\cdots!i_{j_k,p-1}!}, 0\leqslant l\leqslant p-1, 1\leqslant k\leqslant m.$$

Now, we demonstrate the properties of the rotation symmetric orbits whose **forms** are in Δ_k, where $1\leqslant k\leqslant m$ and $\Delta_k = \{\mathrm{I}_{j_k}, \rho_p(\mathrm{I}_{j_k}), \cdots, \rho_p^{p-1}(\mathrm{I}_{j_k})\}$, and we have Theorem 1.

Proof of Theorem 1. With the help of Lemmas 3 and 4, we only need to prove that the first column of $\mathbf{Q}$, i.e., $\mathbf{a}_1$, which is an OA$(pq, 1, p, 1)$. This implies that each symbol $k\in\mathbb{F}_p$ occurs the same number of times in the first column $\mathbf{a}_1$.

Suppose that $\mathrm{I}_{j_k} = (i_0, i_1, \cdots, i_{p-1})$. According to the definition of ρ_p^l, we know that $\rho_p^l(\mathrm{I}_{j_k}) = (i_l, i_{l+1}, \cdots, i_{p-1}, i_0, i_1, \cdots, i_{l-1})$, $l\in\mathbb{F}_p$. Notice that Q_l can be written as

$$Q_l = \begin{pmatrix} x_0 & x_1 & \cdots & x_{q-2} & x_{q-1} \\ x_1 & x_2 & \cdots & x_{q-1} & x_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{q-1} & x_0 & \cdots & x_{q-3} & x_{q-2} \end{pmatrix} = (\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_q),$$

we know that Q_l is symmetric, where $\mathbf{b}_1$ is the first column of Q_l. It is obvious that $\mathbf{b}_1$ contribute i_l number of 0, i_{l+1} number of 1, i_{l+2} number of 2, $\cdots$, i_0 number of $p-l$, i_1 number of $p-l+1$, $\cdots$,i_{l-1} number of $p-1$ for the first column of $\mathbf{Q}$. Let l run over $\mathbb{F}_p$. Then it is easy to show that the number of times, which 0 occurs in column vector $\mathbf{a}_1$, is $\sum\limits_{l=0}^{p-1} i_l = q$. Similarly, we know that the number of times of each $l\in\mathbb{F}_p$ occurs in the column vector $\mathbf{a}_1$ is also q. This result implies that the column vector $\mathbf{a}_1$ is an OA$(pq, 1, p, 1)$, that is to say, each symbol $l\in\mathbb{F}_p$ occurs the same times in $\mathbf{a}_1$. This completes the proof of Theorem 1.

By Theorem 1, we choose an rotation symmetric orbit from $RSO(\rho_p^l(\mathrm{I}_{j_k}))$ for every $l\in\mathbb{F}_p$ respectively, and regard these p different rotation symmetric orbits as $M_{k,1}$. If we do this step repeatedly, until all the rotation symmetric orbits in $RSO(\rho_p^l(\mathrm{I}_{j_k}))$ are arranged, then we have n_k different OAs$(pq, q, p, 1)$, which are denoted as $M_{k,1}, M_{k,2}, \cdots, M_{k,n_k}$. If we perform the same steps for every $1\leqslant k\leqslant m$, then we altogether have $\sum_{k=1}^{m} n_k (= \frac{p^{q-1}-1}{q})$ different OAs$(pq, q, p, 1)$.

Notice that $\frac{p^{q-1}-1}{q}$ is not a multiple of p, so we can not construct q-variable 1-resilient rotation symmetric functions if we do not partition anyone of the above OAs$(pq, q, p, 1)$. In order to overcome the obstacle, our main idea is to divide some OAs$(pq, q, p, 1)$ obtained above into p different groups $V_l(l\in\mathbb{F}_p)$ in average. We partition the rest of OAs$(pq, q, p, 1)$ into long rotation symmetric orbits, and combine each short rotation symmetric orbit with the same number of special rotation symmetric orbits into an orthogonal array of strength 1, then p different orthogonal arrays of strength 1 with the same number of rows are constructed. At last, we place these p different orthogonal arrays of strength 1 into p different groups $V_l(l\in\mathbb{F}_p)$.

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 $w = \frac{r\cdot q+1}{p} = p^{q-2} - q\cdot g$. Now we firstly need to find r special OAs$(pq, q, p, 1)$, and partition them into rp different rotation symmetric orbits. In what follows, we assign the rp different rotation symmetric orbits again, and then propose a method to reach the goal. The following theorem is important in our method.

Proof of Theorem 2. Without loss of generality, suppose that $1\leqslant k_1 < k_2 < \cdots < k_t\leqslant m$, we construct p different OAs$(rq+1, q, p, 1)$, i.e., $B_0, B_1, \cdots, B_{p-1}$, such that $\mathbf{e}_{q,i}\in B_i$, $B_i\bigcap B_j = \phi$ for $i\neq j$, and each B_i contains r number of long rotation symmetric orbits. Firstly, we construct B_0 according to the following steps:

Step 1. We choose l_1 number of OAs$(pq, q, p, 1)$ from the set $\{M_{k_1,1}, M_{k_1,2}, \cdots, M_{k_1,n_{k_1}}\}$, without loss of generality, we denote them as $M_{k_1,1}, M_{k_1,2}, \cdots, M_{k_1,l_1}$. We choose l_2 number of OAs$(pq, q, p, 1)$ from $\{M_{k_2,1}, M_{k_2,2}, \cdots, M_{k_2,n_{k_2}}\}$, and denote them as $M_{k_2,1}, M_{k_2,2}, \cdots, M_{k_2,l_2}$. $\cdots, \cdots$. We choose l_t number of OAs$(pq, q, p, 1)$ from the set $\{M_{k_t,1}, M_{k_t,2}, \cdots, M_{k_t,n_{k_t}}\}$, and denote them as $M_{k_t,1}, M_{k_t,2}, \cdots, M_{k_t,l_t}$.

Step 2. Pick out $\mathbf{e}_{q,0}$.

Step 3. Based on the step 1, we pick out the x_1-**form** rotation symmetric orbit from $M_{k_1,1}$, and pick out the x_2-**form** rotation symmetric orbit from $M_{k_1,2}$, $\cdots$, and pick out the x_{l_1}-**form** rotation symmetric orbit from M_{k_1,l_1}.

Step 4. We pick out the x_{l_1+1}-**form** rotation symmetric orbit from $M_{k_2,1}$, and pick out the x_{l_1+2}-**form** rotation symmetric orbit from $M_{k_2,2}$, $\cdots$, and pick out the $\mathsf{x}_{l_1+l_2}$-**form** rotation symmetric orbit from M_{k_2,l_2}.

So on and so forth, $\cdots, \cdots, \cdots$

Step $t+2$. We pick out the x_{r-l_t+1}-**form** rotation symmetric orbit from $M_{k_t,1}$, and pick out the x_{r-l_t+2}-**form** rotation symmetric orbit from $M_{k_t,2}$, $\cdots$, and pick out the x_r-**form** rotation symmetric orbit from M_{k_t,l_t}.

All the rotation symmetric orbits picked out from Step 2 to Step $t+2$ are regarded as B_0. The equation system (1) means that r number of rotation symmetric orbits picked out from Step 3 to Step $t+2$ contribute $w-1$ number of 0s and w number of js for the first column of B_0 for $1 \leqslant j \leqslant p-1$, adding the vector $\mathbf{e}_{q,0}$ to B_0, then B_0 is now an OA$(rq+1, q, p, 1)$.

Notice that if $\mathbf{X} = (\mathrm{X}_0, \mathrm{X}_1, \cdots, \mathrm{X}_{p-1})$ is a solution of the following equation system

$$(1)\begin{cases} \mathbf{e}_{r,1}\mathbf{X} = \mathbf{e}_{p,w} - \mathbf{e}_1, \\ \mathbf{X}\mathbf{e}_{p,1}^{\top} = \mathbf{e}_{r,q}^{\top}, \end{cases}$$

then $(\mathrm{X}_{p-i+1}, \mathrm{X}_{p-i+2}, \cdots, \mathrm{X}_{p-1}, \mathrm{X}_0, \mathrm{X}_1, \cdots, \mathrm{X}_{p-i})$ is a solution of the following equation system

$$(i)\begin{cases} \mathbf{e}_{r,1}\mathbf{X} = \mathbf{e}_{p,w} - \mathbf{e}_i, \\ \mathbf{X}\mathbf{e}_{p,1}^{\top} = \mathbf{e}_{r,q}^{\top}, \end{cases}$$

and vice visa, where X_i is the i-th colmn vector of $\mathbf{X}$.

In what follows, we regard $(\mathrm{X}_{p-i+1}, \mathrm{X}_{p-i+2}, \cdots, \mathrm{X}_{p-1}, \mathrm{X}_0, \mathrm{X}_1, \cdots, \mathrm{X}_{p-i})$ as $\mathbf{X}$ above, do the Step 3 to Step $t+2$ repeatedly, and pick out $\mathbf{e}_{q,i}$, and regard these rotation symmetric orbits as B_i, where $1 \leqslant i \leqslant p-1$. By the same way, we know that B_i is also an OA$(rq+1, q, p, 1)$. That completes the proof of the theorem.

Remark 1. In fact, Theorem 2 motivates us to find r special OAs$(pq, q, p, 1)$ through the solutions of the above equation system (i), and we partition them to rp different long rotation symmetric orbits. We choose r different long rotation symmetric orbits from them and a short rotation symmetric orbit to make up an OA$(rq+1, q, p, 1)$. By Theorem 2, we can construct the other $p-1$ number of OAs$(rq+1, q, p, 1)$, each OA$(rq+1, q, p, 1)$ contains a short rotation symmetric orbit. As we know that the equation system (1) has μ different solutions, i.e., $\mathbf{X}^1, \mathbf{X}^2, \cdots, \mathbf{X}^{\mu}$, where

$$\mathbf{X}^s = \begin{pmatrix} x_{1,0}^s & x_{1,1}^s & \cdots & x_{1,p-1}^s \\ x_{2,0}^s & x_{2,1}^s & \cdots & x_{2,p-1}^s \\ \vdots & \vdots & \vdots & \vdots \\ x_{r,0}^s & x_{r,1}^s & \cdots & x_{r,p-1}^s \end{pmatrix} = \begin{pmatrix} \mathsf{x}_1^s \\ \mathsf{x}_2^s \\ \vdots \\ \mathsf{x}_r^s \end{pmatrix}, 1 \leqslant s \leqslant \mu.$$

If $\mathbf{P}$ is an $r \times r$ permutation matrix, then $\mathbf{X}^s$ and $\mathbf{P}\mathbf{X}^s$ are seen as same in this paper. The row vectors of $\mathbf{X}^s$ actually are the **form**s of the rotation symmetric orbits that we need to pick out, where x_k^s is the k-th row vector of $\mathbf{X}^s$, $1 \leqslant k \leqslant r$.

Now, we assign the rest $\frac{p^{q-1}-1}{q} - r$ different OAs$(pq, q, p, 1)$ to p groups $A_0, A_1, \cdots, A_{p-1}$, in the following, we propose an efficient method to attain the purpose.

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

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

If the equation system

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

has λ different solutions as follows:

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

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

Remark 2. Actually, the solutions of the equation system Θ_r are the schemes to arrange the rest $\frac{p^{q-1}-1}{q} - r$ different OAs$(pq, q, p, 1)$. It is easily shown that different solutions deduce different q-variable 1-resilient RSFs. From Theorem 2 and the analysis above, it is showed that $(l_1, l_2, \cdots, l_t)$ is determined by the corresponding solution of equation system (1). Then, we can get all the solutions of the corresponding equation system (1) and Θ_r respectively by using computer program. We observed that it has many cases to count the q-variable 1-resilient RSFs by utilizing the solutions of equations system Θ_r under the condition that some of $l_1, l_2, \cdots, l_t$ are large, and it is hard to get the total number of the methods to arrange the corresponding rotation symmetric orbits according to the **form**s of the rotation symmetric orbits and the solutions of Θ_r.

But if $t = r$, which means that $l_1 = l_2 = \cdots = l_t = 1$, then we have Theorem 3.

Proof of Theorem 3. Suppose that X is a solution of the equation system (1). By Theorem 2, the row vectors of $\mathbf{X}$ are sorted to the following t different classes:

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

Without loss of generality, suppose that $1 \leqslant k_1 < k_2 < \cdots < k_t \leqslant m$. If $l_1 = l_2 = \cdots = l_t = 1$, then $t = r$. We know that the following equation system

$$\Theta_r : \begin{cases} \mathbf{e}_{p,1}\mathbf{Y} = (n_1, n_2, \cdots, n_{k_1-1}, n_{k_1} - 1, n_{k_1+1}, \cdots, \\ \qquad \cdots, n_{k_2-1}, n_{k_2} - 1, n_{k_2+1}, \cdots, n_{k_t-1}, n_{k_t} - 1, n_{k_t+1}, \cdots, n_m) \\ \mathbf{Y}\mathbf{e}_{m,1}^{\top} = \mathbf{e}_{p,g}^{\top}, \text{where } g = \frac{p^{q-1}-1-qr}{pq}. \end{cases}$$

has λ different solutions $\mathbf{Y}^s(1 \leqslant s \leqslant \lambda)$. Now we give a method to construct q-variable 1-resilient RSFs over $\mathbb{F}_p$ by using the solutions of equation systems (1) and Θ_r according to the following method:

Case 1. If $j \in \{1, 2, \cdots, m\} \setminus J$, then we firstly divide n_j different matrices in the sets $\{M_{j,1}, M_{j,2}, \cdots, M_{j,n_j}\}$ into p groups $A_0, A_1, \cdots, A_{p-1}$ such that A_l contains $y_{j,l}^s$ number of matrices, where $l \in \mathbb{F}_p, 1 \leqslant j \leqslant m, j \notin J$. Let j run over the set $\{1, 2, \cdots, m\} \setminus J$, then we know that the total number of ways to do this step is

$$\prod_{k=1, k\notin J}^{m} \frac{n_k!}{y_{k,0}^s! \cdot y_{k,1}^s! \cdots y_{k,p-1}^{\nu}!}.$$

Case 2. If $j \in J = \{k_1, k_2, \cdots, k_r\}$, then we choose a matrix from $\{M_{j,1}, M_{j,2}, \cdots, M_{j,n_j}\}$ for each $j \in J$. Without loss of generality, we denote the r different chosen matrices as $M_{k_1,1}, M_{k_2,1}, \cdots, M_{k_r,1}$, and these matrices contain rp different rotation symmetric orbits. Since X is a solution of the equation system (1), we divide the rp different rotation symmetric orbits into p groups $B_0, B_1, \cdots, B_{p-1}$ such that rotation symmetric orbits in each group consist of an $\mathrm{OA}(rq + 1, q, p, 1)$ by the following steps:

Step 1. Pick out the x_1-**form** rotation symmetric orbit from $M_{k_1,1}$, and pick out the x_2-**form** rotation symmetric orbit from $M_{k_2,1}, \cdots$, and pick out the x_r-**form** rotation symmetric orbit from $M_{k_r,1}$, along with the vector $\mathbf{e}_{q,0}$, we regard the vectors in these rotation symmetric orbits as the vectors of B_0. By Theorem 2, we know that B_0 is an $\mathrm{OA}(rq + 1, q, p, 1)$.

Step 2. Pick out the $\rho_p(\mathsf{x}_1)$-**form** rotation symmetric orbit from $M_{k_1,1}$, and pick out the $\rho_p(\mathsf{x}_2)$-**form** rotation symmetric orbit from $M_{k_2,1}, \cdots$, and pick out the $\rho_p(\mathsf{x}_r)$-**form** rotation symmetric orbit from $M_{k_r,1}$, along with the vector $\mathbf{e}_{q,p-1}$, regarding the vectors in these rotation symmetric orbits as the vectors of B_{p-1}. By Theorem 2, we know that B_{p-1} is an $\mathrm{OA}(rq + 1, q, p, 1)$.

So on and so forth, $\cdots, \cdots, \cdots$

Step p. Pick out the $\rho_p^{p-1}(\mathsf{x}_1)$-**form** rotation symmetric orbit from $M_{k_1,1}$, and pick out the $\rho_p^{p-1}(\mathsf{x}_2)$-**form** rotation symmetric orbit from $M_{k_2,1}, \cdots$, and pick out the $\rho_p^{p-1}(\mathsf{x}_r)$-**form** rotation symmetric orbit from $M_{k_r,1}$, along with the vector $\mathbf{e}_{q,1}$, regarding the vectors in these rotation symmetric orbits as the vectors of B_1. By Theorem 2, we know that B_1 is an $\mathrm{OA}(rq + 1, q, p, 1)$.

Step $p + 1$. We now divide the matrices in the set $\bigcup_{j\in J}\bigcup_{i=2}^{n_j}\{M_{j,i}\}$ into p groups by the solution Y^s. For each $j \in J$, we choose $y_{j,l}^s$ matrices from $\bigcup_{i=2}^{n_j}\{M_{j,i}\}$ and place them into A_l, where $0 \leqslant l \leqslant p - 1$.

Step $p + 2$. Select an A_i from $\{A_0, A_1, \cdots, A_{p-1}\}$, select a B_j from $\{B_0, B_1, \cdots, B_{p-1}\}$ and regard V_l as $A_i \cup B_j$ for each l, where $i, j, l \in \mathbb{F}_p$.

Now, we consider the total number of q-variable 1-resilient RSFs over $\mathbb{F}_p$ from Step 1 to Step $p + 2$. As we know, two rotation symmetric orbits whose **form**s are same can be seen as identical in the constructions of q-variable 1-resilient RSFs over $\mathbb{F}_p$. Notice that the implications of the solution Y^s, and the p different rotation symmetric orbits in each $M_{j,1}(j \in J)$ must be in different V_l, we know that the total number of methods to arrange the rotation symmetric orbits whose **form**s are in $\Delta_j(j \in J)$ is

$$\frac{(n_j!)^p}{\prod_{l=0}^{p-1}\left((y_{j,l}^s!)^{p-1}(y_{j,l}^s + 1)!\right)} = \frac{(n_j!)^p}{\prod_{l=0}^{p-1}\left((y_{j,l}^s!)^{p}(y_{j,l}^s + 1)\right)}.$$

On the other hand, under the conditions of Theorem 3, if $\mathbf{Y}^{s_1}$ and $\mathbf{Y}^{s_2}$ are two different solutions of the equation system Θ_r, then the methods to partition the space $\mathbb{F}_p^q$ according to our method are different.

By the multiplication principle, we know that the total number of the methods to partition the space $\mathbb{F}_p^q$ into the p different disjoint sets satisfying $\mathbb{F}_p^q = V_0 \cup V_1 \cup V_2 \cup \cdots \cup V_{p-1}$ is

$$E_sF_s = \sum_{s=1}^{\lambda}\left(\prod_{j\in J}\frac{(n_{k_j}!)^p}{\prod_{l=0}^{p-1}(y_{j,l}^s!)^{p-1}(y_{j,l}^s + 1)!}\right)\left(\prod_{k=1, k\notin J}^{m}\frac{n_k!}{y_{k,0}^s! \cdot y_{k,1}^s! \cdots y_{k,p-1}^{\nu}!}\right)^{p}.$$

Define a function $f(x)$ such that $\{x|f(x)=l\}=V_l$, where $l\in\mathbb{F}_p$. It is obvious that $f(x)$ is a q-variable 1-resilient RSFs over $\mathbb{F}_p$, and the total number of q-variable 1-resilient RSFs over $\mathbb{F}_p$ constructed by our method is

$$\boldsymbol{N}=\sum_{s=1}^{\lambda}p!E_sF_s=\sum_{s=1}^{\lambda}p!\left(\prod_{j\in J}\frac{(n_{k_j}!)^p}{\prod_{l=0}^{p-1}(y_{j,l}^s!)^{p-1}(y_{j,l}^s+1)!}\right)\left(\prod_{k=1,k\notin J}^{m}\frac{n_k!}{y_{k,0}^s!\cdot y_{k,1}^s!\cdots y_{k,p-1}^{\nu}!}\right)^p.$$

Proof of Corollary 1. If $r=1$, then $w=\frac{r\cdot q+1}{p}=\frac{q+1}{p}$ is an integer. Without loss of generality, suppose that $(w-1,w,w,\cdots,w)=\mathrm{I}_{j_{k_1}}\in\Delta_{k_1}$, a matrix chosen from $\{M_{k_1,1},M_{k_1,2},\cdots,M_{k_1,n_{k_1}}\}$, say $M_{k_1,1}$. Now, we divide the other $\frac{p^{q-1}-1-q}{q}$ number of OAs$(pq,q,p,1)$ into p groups. According to the method proposed above, equation system Θ_r is simplified as

$$\Theta_1:\begin{cases}\mathbf{e}_{p,1}\mathbf{Y}=(n_1,n_2,\cdots,n_{k_1-1},n_{k_1}-1,n_{k_1+1},\cdots,n_m),\\ \mathbf{Y}\mathbf{e}_{m,1}^{\top}=\mathbf{e}_{p,g}^{\top},\text{where }\ g=\frac{p^{q-1}-qr-1}{pq}=\frac{p^{q-1}-q-1}{pq}.\end{cases}$$

By the proof of Theorem 3, we know that the total number of q-variable 1-resilient RSFs over $\mathbb{F}_p$ constructed by our method is

$$\boldsymbol{N}=\sum_{\nu=1}^{\mu}\frac{p!}{\prod\limits_{j=0}^{p-1}(y_{k_1,j}^{\nu}+1)}\Big(\prod_{l=1}^{m}\frac{n_l!}{y_{l,0}^{\nu}!\cdot y_{l,1}^{\nu}!\cdots y_{l,p-1}^{\nu}!}\Big)^p.$$

Remark 3. In fact, we can construct a class of q-variable 1-resilient RSFs over $\mathbb{F}_p$ by Corollary 1 for any q and p such that $q+1\equiv 0(mod\ p)$. For example, we can construct a class of 19-variable 1-resilient RSFs over $\mathbb{F}_5$ by Corollary 1.

Appendix C An illustrative example

From the method proposed in Appendix B, we note that if the characteristic of the finite field $\mathbb{F}_p$ is very small, then the number of rows of the matrix $\mathbf{X}$ in Theorem 2 is also small. In order to demonstrate the method proposed in Theorem 3, we give a simple example as follows:

Example 1. Consider the constructions of 5-variable 1-resilient rotation symmetric functions over $\mathbb{F}_3$.

Let $p=3,q=5$. Then the total number of the **forms** of the long rotation symmetric orbits is $N=C(p+q-1,q)-p=18$, and that the number of the long rotation symmetric orbits is $h_{q,p}=p\frac{p^{q-1}-1}{q}=48$. We obtain all these **forms** through the equation $i_0+i_1+i_2=5$ as follows:

$$(0,1,4),(1,4,0),(4,0,1),(0,2,3),(2,3,0),(3,0,2),(0,4,1),(4,1,0),(1,0,4),$$
$$(0,3,2),(3,2,0),(2,0,3),(1,1,3),(1,3,1),(3,1,1),(1,2,2),(2,2,1),(2,1,2).$$

Note that (0,0,5),(0,5,0),(5,0,0) correspond to three short rotation symmetric orbits, we omit here. Let the permutation ρ_3 act on the above 18 solutions of the equation $i_0+i_1+i_2=5$. For convenience and simplicity, we assume that $j_k\in\{1,2,3,4,5,6\}$. Then we can obtain the following equivalent classes:

$$\Delta_1=\{(0,1,4),(1,4,0),(4,0,1)\},\Delta_2=\{(0,2,3),(2,3,0),(3,0,2)\},\Delta_3=\{(0,4,1),(4,1,0),(1,0,4)\},$$
$$\Delta_4=\{(0,3,2),(3,2,0),(2,0,3)\},\Delta_5=\{(1,1,3),(1,3,1),(3,1,1)\},\Delta_6=\{(1,2,2),(2,2,1),(2,1,2)\},$$

and compute $n_1=\frac{(5-1)!}{0!1!4!}=1,n_2=\frac{(5-1)!}{0!2!3!}=2,n_3=\frac{(5-1)!}{0!4!1!}=1,n_4=\frac{(5-1)!}{0!3!2!}=2,n_5=\frac{(5-1)!}{1!1!3!}=4,n_6=\frac{(5-1)!}{1!2!2!}=6.$

Step 1. calculate $r=\frac{3^{5-1}-1}{5}-3g=16-3g=1$, where $g=5$. Where $r=1$ means that we need to pick three rotation symmetric orbits whose **form**s are in the same set Δ_{j_k}.

Step 2. compute $w=\frac{q\cdot r+1}{p}=p^{q-2}-q\cdot g=2$.

Step 3. $\mathbf{X}=(x_{1,0},x_{1,1},x_{1,2})$, then we obtain a unique solution $\mathbf{X}=\mathsf{x}_1=(1,2,2)$. Firstly, we choose a (1,2,2)-**form** rotation symmetric orbit and pick out $\mathbf{e}_{3,0}$, the vectors in which make of an OA(6,5,3,1). Secondly, we choose a (2,1,2)-**form** rotation symmetric orbit and pick out $\mathbf{e}_{3,1}$, the vectors in these two rotation symmetric orbits which make of an OA(6,5,3,1). At last, we choose a (2,2,1)-**form** rotation symmetric orbit and pick out $\mathbf{e}_{3,2}$, which form an OA(6,5,3,1), then we have $n_6-1=5$.

Step 4. Let

$$\begin{cases}\mathbf{e}_{3,1}\mathbf{Y}=(1,2,1,2,4,5),\\ \mathbf{Y}\mathbf{e}_{6,1}^{\top}=(5,5,5)^{\top},\end{cases}\quad\text{where }\ \mathbf{Y}=\begin{pmatrix}y_{1,0}&y_{2,0}&y_{3,0}&y_{4,0}&y_{5,0}&y_{6,0}\\ y_{1,1}&y_{2,1}&y_{3,1}&y_{4,1}&y_{5,1}&y_{6,1}\\ y_{1,2}&y_{2,2}&y_{3,2}&y_{4,2}&y_{5,2}&y_{6,2}\end{pmatrix},$$

if we solve the above equation system, then we have a solution as follows:

$$\mathbf{Y}=\begin{pmatrix}1&1&0&0&2&1\\ 0&0&1&1&1&2\\ 0&1&0&1&1&2\end{pmatrix}.$$

In fact, this solution deduces a scheme to construct 5-variable 1-resilient RSFs over $\mathbb{F}_3$. By Theorem 3 and Corollary 1, the number of 5-variable 1-resilient RSFs over $\mathbb{F}_3$ constructed according to $\mathbf{Y}$ is

$$3!\left(\frac{1!}{1!0!0!}\cdot\frac{2!}{1!0!1!}\cdot\frac{1!}{0!1!0!}\cdot\frac{2!}{0!1!1!}\cdot\frac{4!}{2!1!1!}\right)^3\cdot\left(\frac{6!}{3!2!1!}\cdot\frac{6!}{2!3!1!}\cdot\frac{6!}{2!2!2!}\right)=214990848000.$$

Notice that the number of 5-variable 1-resilient RSFs over $\mathbb{F}_3$ is large, although we can obtain other q-variable 1-resilient RSFs by the other solution Y^{ν}, we can not obtain all the 5-variable 1-resilient RSFs over $\mathbb{F}_3$ by this method, so we do not give all the solutions of the above equation system here.

Appendix D Conclusion

In this letter, a method to construct q-variable 1-resilient RSFs over $\mathbb{F}_p$ is presented , and a sufficient condition to construct q-variable 1-resilient RSFs is given, where p and q are different odd prime numbers. It is efficient to construct a class of q-variable 1-resilient RSFs according to our method, but it is difficult for us to get all the solutions of the equation systems if p and q are too large. It can be regarded as an instance of *Knapsack Problem*, which is a so-called NP-complete problem. The construction of 1-resilient RSFs on given number of variables remains to be an open problem.

References

1 Filiol, E., Fontaine, C., Highly nonlinear balanced Boolean functions with a good correlation-immunity, in:Proceedings of EUROCRYPT'98, in: Lecture Notes in Comput.Sci., vol.1403, 1998, pp. 475-488.

2 Pieprzyk, J., Qu, C.X., Fast hashing and rotation symmetric functions, J. Univers. Comput. Sci., vol. 5, no.1, pp. 20-31, 1999.

3 Stănică, P., Maitra, S., Clark, J., Results on rotation symmetric bent and correlation immune Boolean functions, Fast software encryption workshop (FSE 2004), New Delhi, India, LNCS3017. Springer Verlag, 2004, 161-177.

4 Kavut, S. Results on rotation symmetric S-boxes, Information Science, 201, 93-113(2012).

5 Gao, G., Cusick, T.W., Liu, W. Families of rotation symmetric functions with useful cryptographic properties, IET Information Security, vol.8, Iss.6, pp. 297-302, 2014.

6 Gao, G., Zhang, X., Liu, W., Carlet, C., Constructions of quadratic and cubic rotation symmetric bent Boolean functions, IEEE Trans. Inform. Theory, vol.58, no.7, pp.4908-4913, 2012.

7 Carlet, C., Gao, G., Liu, W., A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semibent functions, J. Combin. Theory Ser. A, vol.127, pp.161-175, 2014.

8 Carlet, C., Gao, G., Liu, W., Results on constructions of rotation symmetric bent and semibent functions, K.-U. Schmidt and A. Winterhof(Eds.): SETA 2014, LNCS 8865, pp.21-33, 2014. DOI: 10.1007/978-3-319-12325-7-2, Springer International Publishing Switzerland 2014.

9 Kavut, S., Maitra, S., Sarkar, S., Yucel, M.D., Enumeration of 9-variable Rotation symmetric Boolean functions having nonlinearity>240, In: INDOCRYPT 2006, 2006 (LNCS, 4329), Springer-Verlag, pp. 266-279. Available at http://eprint.iacr.org/2006/249.

10 Carlet, C., Dalai, D.K., Gupta, K.C., et al., Algebraic immunity for cryptographically significant Boolean functions: analysis and construction, IEEE Trans. Inf. Theory, vol.52, no.7, pp. 3105-3121, 2006.

11 Kavut, S., Maitra, S., Yücel, M.D., Search for Boolean functions with excellent profiles in the rotation symmetric class, IEEE Trans. Inf. Theory, vol.53, no.5, pp.1743-1751, May 2007.

12 Stănică, P., Maitra, S., Rotation symmetric Boolean functions count and cryptographic properties, Discrete Applied Mathematics, vol.156, pp.1567-1580, 2008.

13 Fu, S., Qu, L., Li, C., Sun, B., Balanced rotation symmetric Boolean functions with maximum algebraic immunity, IET Information Security, vol.5, no.2, pp.93-99, 2011.

14 Su, S., Tang, X., Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity, Des. Codes Cryptogr.(2014)71:183-199.

15 Zhang, Y., Liu, M., Lin, D., On the immunity of rotation symmetric Boolean functions against fast algebraic attacks, Discrete Applied Mathematics, Vol.162, pp.17-27, 2014.

16 Fu, S., Li, C., Matsuura, K., Qu, L., Construction of even-variable rotation symmetric Boolean functions with maximum algebraic immunity. Sci. China Inf. Sci., 2013, 56(3):032106, http://link. springer. com/article/10.1007/s11432-011-4350-4.

17 Sarkar, P., Maitra, S., Balancedness and correlation immunity of symmetric Boolean functions, Discrete Math., 2007, 307, pp. 2351-2358.

18 Peng, J., Kan, H.B., Constructing correlation immune symmetric Boolean functions. IEICE Transactions on Fundamentals, vol. E94-A, No.7, pp.1591-1596, 2011.

19 Du, J., Wen, Q., Zhang, J., Pang, S., Constructions of resilient rotation symmetric Boolean functions on given number of variables, IET Information Security, 2014, Vol.8, Iss.5, pp.265-272.

20 Du, J., Pang, S., Wen, Q., Liao, X., Construction and count of 1-resilient rotation symmetric Boolean functions on p^r variables, Chinese Journal of Electronics, 2014, Vol.23, No.4, pp.816-820.

21 Wu, C.K., Dawson, E., Correlation immunity and resiliency of symmetric Boolean functions, Theor. Comput. Sci., vol.312, pp.321-335, 2004.

22 Canteaut, A., Videau, M., Symmetric Boolean functions, IEEE Trans. Inf. Theory, vol.51, no.8, pp.2791-2811, 2005.

23 Cusick, T.W., Li, Y., Stânicâ, P., Balanced symmetric functions over $GF(p)$, IEEE Trans. Inform. Theory, vol.54, no.3, pp.1304-1307, 2008.

24 Li, Y., Results on rotation symmetric polynomials over $GF(p)$, Information Sciences, vol.178, pp.280-286, 2008.

25 Li, Y., Cusick, T W., Linear structure of symmetric functions over finite fields, Information Processing Letters, 97(2006)124-127.

26 Ke, P., Huang, L., Zhang, S., Improved lower bound on the number of balanced symmetric functions over $GF(p)$, Information Sciences, vol.179, pp.682-687, 2009.

27 Fu, S., Li, C., Qu, L., Dong, D., On the number of rotation symmetric functions over $GF(p)$, Mathematical and Computer Modelling, vol.55(1-2), pp.142-150, 2012.

28 Stănică, P., Maitra, S., A constructive count of rotation symmetric functions, Information Processing Letters, vol.88, pp. 299-304, 2003.

29 Zhang, W., Pasalic, E., Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes, IEEE Trans. Inform. Theory, vol.60, no.3, pp.1638-1651, 2014.

30 Zhang, W., Jiang, F., Tang, D., Construction of highly nonlinear resilient Boolean functions satisfying strict avalanche criterion. Sci. China Inf. Sci., 2014, 57(4):049101, http://link. springer. com/article/10.1007/s11432-014-5073-0.

31 Zhang, W., Pasalic, E., Generalized Maiorana-McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties, IEEE Trans. Inform. Theory, vol.60, no.10, pp.6681-6695, 2014.