7 元旋转对称 2−弹性函数的构造

杜皎[1,2]，李琳[1,2]，赵紫薇[1,2]，李月月[1,2]，王天银[1,3]

（1. 河南师范大学数学与信息科学学院，河南 新乡 453007；
2. 北京邮电大学网络与交换技术国家重点实验室，北京 100876；
3. 洛阳师范学院数学科学学院，河南 洛阳 471934）

摘 要：基于旋转对称轨道的数对分布矩阵的性质，给出了所有 7 元旋转对称 2−弹性函数的具体构造。结果表明，在 $\mathbb{F}_2^7$ 上有且仅有 280 个非线性旋转对称 2−弹性函数。进一步地，对于任意的奇数 k，在 $\mathbb{F}_2^{7k}$ 上至少有 280 个非线性旋转对称 2−弹性函数。

关键词：密码学；旋转对称函数；弹性函数；支撑矩阵；数对分布矩阵

中图分类号：TN918.1

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2024007

Concrete constructions of 2-resilient rotation symmetric Boolean functions with 7 variables

DU Jiao[1,2], LI Lin[1,2], ZHAO Ziwei[1,2], LI Yueyue[1,2], WANG Tianyin[1,3]

1. College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China
2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
3. Faculty of Mathematical Sciences, Luoyang Normal University, Luoyang 471934, China

Abstract: Based on the properties of the 2-tuples distribution matrix of the rotation symmetric orbits, all 7-variable 2-resilient rotation symmetric Boolean functions were constructed concretely. The results show that there are only 280 nonlinear 2-resilient rotation symmetric Boolean functions over $\mathbb{F}_2^7$. Furthermore, there are at least 280 nonlinear 2-resilient rotation symmetric Boolean functions over $\mathbb{F}_2^{7k}$ for any odd number k.

Keywords: cryptography, rotation symmetric function, resilient function, support matrix, 2-tuples distribution matrix

0 引言

在对称密码体制中，具有各种密码学性质的布尔函数和向量值函数被用来设计密码算法，以抵抗各种攻击方法，比如差分攻击、线性密码攻击、相关攻击、代数攻击等[1]。寻找和构造同时具有多个密码学性质的布尔函数是当前对称密码学领域中一个极具理论意义和应用价值的挑战性课题，吸引了众多学者，出现了一批研究成果[2-4]。

旋转对称布尔函数是一种在输入变量周期性旋转变化时函数值保持不变的布尔函数类，对称布尔函数是其子类[2-7]。1999 年，Pieprzyk 等[8]将旋转对称布尔函数用于 MD4、MD5 和 HAVAL 等密码算法的快速实现中。Kavut 等[9-10]在旋转对称函数类中找到了非线性度 241 的 9 元布尔函数，解决了一个近 30 年的公开问题。进一步的研究表明，

收稿日期：2023−09−08；**修回日期：**2023−11−28

通信作者：王天银，wangtianyin79@163.com

基金项目：国家自然科学基金资助项目（No.62372157, No.62272208, No.62172196, No.12001173, No.11971004）；北京邮电大学网络与交换技术国家重点实验室开放基金资助项目（No.SKLNST-2022-1-01）

Foundation Items: The National Natural Science Foundation of China (No.62372157, No.62272208, No.62172196, No.12001173, No.11971004), The Open Foundation of State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications (No.SKLNST-2022-1-01)

旋转对称布尔函数可以同时具有多个良好的密码学性质，比如平衡性、相关免疫性、高非线性度、最优代数免疫性和较高的代数次数等[11]。因此，旋转对称布尔函数的研究受到越来越多的关注，关于旋转对称布尔函数的研究成果也越来越多。文献[12-15]研究了旋转对称 Bent 函数的构造，文献[2,16]研究了旋转对称最优代数免疫函数的构造，文献[2-4,17]研究了平衡的旋转对称函数的构造，文献[18-25]研究了旋转对称 1−弹性函数和 2−弹性函数的构造。长期以来，7 元非线性度 56 的 2−弹性函数的构造问题是一个极端困难的组合问题，文献[7]通过计算机程序获得了 72 个非线性度和代数次数最优的 7 元旋转对称 2−弹性函数。为了进一步研究 7 元旋转对称 2−弹性函数的密码学性质，本文基于旋转对称轨道的数对分布矩阵，具体给出了所有的 7 元旋转对称 2−弹性函数。

1　预备知识

假设 $\mathbb{F}_2^n$ 表示 $\mathbb{F}_2=\{0,1\}$ 上的 n 维线性空间，$|T|$ 表示集合 T 中元素的个数，为了叙述方便，本文中 T 既可以表示由维数相同的行向量构成的集合，也可以表示由集合 T 中行向量构成的矩阵（不考虑顺序）。记 $\mathrm{wt}(\boldsymbol{x})$ 为向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$ 的 Hamming 重量，其中 $\mathrm{wt}(\boldsymbol{x})=x_0+x_1+\cdots+x_{n-1}$。设映射 $f:\mathbb{F}_2^n\to\mathbb{F}_2$ 表示 n 元布尔函数，$\mathbb{B}_n$ 表示全体 n 元布尔函数的集合。对于向量 $\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})\in\mathbb{F}_2^n$，定义 $\boldsymbol{xy}=x_0y_0\oplus x_1y_1\cdots\oplus x_{n-1}y_{n-1}$，其中 $\oplus$ 表示 $\mathbb{F}_2$ 上的加法。$\mathbf{1}_n$ 和 $\mathbf{0}_n$ 分别表示全 1 和全 0 的 n 元行向量，$\boldsymbol{A}\otimes\boldsymbol{B}$ 表示矩阵 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 的 Kronecker 积。

n 元布尔函数 $f(\boldsymbol{x})$ 的 Walsh 值是 $\mathbb{F}_2^n$ 上的实值函数，$f(\boldsymbol{x})$ 在 $\boldsymbol{w}\in\mathbb{F}_2^n$ 处的 Walsh 值表示为

$$W_f(\boldsymbol{w})=\sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{f(\boldsymbol{x})\oplus\boldsymbol{wx}}$$

进一步地，根据 Walsh 值的计算，布尔函数 $f(\boldsymbol{x})$ 的非线性度可以表示为

$$NL(f)=2^{n-1}-\frac{1}{2}\max_{\boldsymbol{w}\in\mathbb{F}_2^n}\left|W_f(\boldsymbol{w})\right| \tag{1}$$

设 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$，对于任意的整数 $0\leqslant d\leqslant n-1$，定义

$$\rho_n^d(x_i)=\begin{cases}x_{i+d}, & i+d\leqslant n-1\\ x_{i+d-n}, & i+d>n-1\end{cases}$$

把 ρ 的定义扩展到 $\mathbb{F}_2^n$ 上，则有 $\rho_n^d(x_0,x_1,\cdots,x_{n-1})=(x_d,x_{d+1},\cdots,x_{d-1})$。

定义 1[5-8]　设函数 $f(\boldsymbol{x})\in\mathbb{B}_n$，向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$，如果对于任意的 $0\leqslant d\leqslant n-1$，都有 $f\left(\rho_n^d(x_0,x_1,\cdots,x_{n-1})\right)=f(x_0,x_1,\cdots,x_{n-1})$，则称 f 为旋转对称布尔函数（RSBF）。

定义 2[23]　设函数 $f(\boldsymbol{x})\in\mathbb{B}_n$，记 $\mathbf{1}_f=\left\{\boldsymbol{x}\in\mathbb{F}_2^n\middle|f(\boldsymbol{x})=1\right\}$。如果 $\left|\mathbf{1}_f\right|=2^{n-1}$，则称 f 是一个平衡函数。$\mathbf{1}_f$ 是 f 的支撑集或支撑矩阵，$\mathbf{1}_f$ 中的行向量被称为 f 的支撑向量。

定义 3[20,23,25]　如果 $f(\boldsymbol{x})\in\mathbb{B}_n$ 的支撑矩阵是正交表 $\mathbf{OA}\left(\left|\mathbf{1}_f\right|,n,2,d\right)$，其中 $d\geqslant 1$，则称 $f(\boldsymbol{x})$ 为 d−相关免疫函数。另外，如果 f 既是 d−相关免疫的又是平衡的，则称 f 是 d−弹性函数。

定义 4[24]　设 $\boldsymbol{O}_n(\boldsymbol{x})=\left\{\rho_n^d(\boldsymbol{x})\middle|\boldsymbol{x}\in\mathbb{F}_2^n,0\leqslant d\leqslant n-1\right\}$ 是向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$ 在循环群 $\boldsymbol{C}_n=\left\{\rho_n^d\middle|0\leqslant d\leqslant n-1\right\}$ 作用下生成的旋转对称轨道（或轨道），则以 $\boldsymbol{O}_n(\boldsymbol{x})$ 中的元素为行向量，总可以得到矩阵

$$\boldsymbol{O}_n(\boldsymbol{x})=\begin{pmatrix}\rho_n^0(\boldsymbol{x})\\ \rho_n^1(\boldsymbol{x})\\ \vdots\\ \rho_n^{l-1}(\boldsymbol{x})\end{pmatrix}=\begin{pmatrix}x_0 & x_1 & \cdots & x_{n-1}\\ x_1 & x_2 & \cdots & x_0\\ \vdots & \vdots & \ddots & \vdots\\ x_{l-1} & x_l & \cdots & x_{l-2}\end{pmatrix}_{l\times n}$$

该矩阵被称为向量 $\boldsymbol{x}$ 的轨道矩阵，其中 $\left|\boldsymbol{O}_n(\boldsymbol{x})\right|=l$，并且 $l|n$。

当 $l=n$ 时，称 $\boldsymbol{O}_n(\boldsymbol{x})$ 为长轨道；否则为短轨道。若 $\left|\boldsymbol{O}_n(\boldsymbol{x})\right|=l<n$，即 $x_i=x_{i+l}=x_{i+2l}=\cdots=x_{i+(s-1)l}$，其中，$\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$，$0\leqslant i\leqslant l-1$，$sl=n$，则

$$\boldsymbol{O}_n(\boldsymbol{x})=\begin{pmatrix}x_0 & x_1 & \cdots & x_{n-1}\\ x_1 & x_2 & \cdots & x_0\\ \vdots & \vdots & \ddots & \vdots\\ x_{l-1} & x_l & \cdots & x_{l-2}\end{pmatrix}=$$

$$\mathbf{1}_s\otimes\begin{pmatrix}x_0 & x_1 & \cdots & x_{l-1}\\ x_1 & x_2 & \cdots & x_0\\ \vdots & \vdots & \ddots & \vdots\\ x_{l-1} & x_0 & \cdots & x_{l-2}\end{pmatrix}$$

引理 1[7,23]　设 n 元旋转对称轨道的总数为 g_n，其中长轨道的总数为 h_n，则 $g_n=\frac{1}{n}\sum_{t|n}\phi(t)2^{\frac{n}{t}}$，其中，

$\phi(t)$ 是欧拉函数；$h_n=\frac{1}{n}\sum_{d|n}\mu(d)2^{\frac{n}{d}}$，$\mu(d)$ 是墨比乌斯函数。当 n 为奇素数时，有 $g_n=\frac{2^n+2(n-1)}{n}$，则 g_n 一定是 4 的倍数。

设向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$ 生成的轨道 $\boldsymbol{O}_n(\boldsymbol{x})=(\boldsymbol{X}_0,\boldsymbol{X}_1,\cdots,\boldsymbol{X}_{n-1})$，其中 $\boldsymbol{X}_i$ 是矩阵 $\boldsymbol{O}_n(\boldsymbol{x})$ 的第 $(i+1)$ 列。易知在任意 $(\boldsymbol{X}_a,\boldsymbol{X}_b)$ 中，数对 01 和 10 出现的频次相同，其中 $0\leqslant a\neq b\leqslant n-1$，再根据文献[20]中定理 2 的证明，可以得到定义 5。

定义 5[23-24] 假设 $\boldsymbol{O}_n(\boldsymbol{x})=(\boldsymbol{X}_0,\boldsymbol{X}_1,\cdots,\boldsymbol{X}_{n-1})$ 是向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$ 生成的轨道。令 b_{i1}、b_{i2}、b_{i3} 分别表示数对 00、01 (10)、11 在矩阵 $(\boldsymbol{X}_0,\boldsymbol{X}_i)$ 中出现的频次，其中 $1\leqslant i\leqslant\left\lfloor\frac{n}{2}\right\rfloor$，则称矩阵 $\boldsymbol{B}_{\boldsymbol{O}_n(\boldsymbol{x})}$ 为轨道 $\boldsymbol{O}_n(\boldsymbol{x})$ 的数对分布矩阵

$$\boldsymbol{B}_{\boldsymbol{O}_n(\boldsymbol{x})}=\begin{pmatrix}b_{11}&b_{12}&b_{13}\\b_{21}&b_{22}&b_{23}\\\vdots&\vdots&\vdots\\b_{\left\lfloor\frac{n}{2}\right\rfloor1}&b_{\left\lfloor\frac{n}{2}\right\rfloor2}&b_{\left\lfloor\frac{n}{2}\right\rfloor3}\end{pmatrix}=(\boldsymbol{b}_1,\boldsymbol{b}_2,\boldsymbol{b}_3)$$

对于向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$，定义 $\bar{\boldsymbol{x}}=(x_0\oplus1,x_1\oplus1,\cdots,x_{n-1}\oplus1)\in\mathbb{F}_2^n$ 为 $\boldsymbol{x}$ 的补向量，易知 $\boldsymbol{O}_n(\bar{\boldsymbol{x}})$ 的数对分布矩阵为 $\boldsymbol{B}_{\boldsymbol{O}_n(\bar{\boldsymbol{x}})}=(\boldsymbol{b}_3,\boldsymbol{b}_2,\boldsymbol{b}_1)$ [23]。另外，如果 T 是若干轨道的并集，则

$$\boldsymbol{B}_{\boldsymbol{T}}=\sum_{\boldsymbol{O}_n(\boldsymbol{x})\subseteq\boldsymbol{T}}\boldsymbol{B}_{\boldsymbol{O}_n(\boldsymbol{x})}$$

由引理 1 可知，$\mathbb{F}_2^7$ 上共有 20 个轨道，其中长轨道 18 个。对这些轨道中的向量按字典序从小到大排列，令每个轨道中的最小向量为其轨道代表元，可得轨道代表元及其数对分布矩阵如表 1 所示。

接下来，本文将根据轨道的数对分布矩阵，对 $\mathbb{F}_2^7$ 上的旋转对称 2–弹性函数进行具体构造。

2 $\mathbb{F}_2^7$ 上旋转对称 2–弹性函数的构造

函数 $f(\boldsymbol{x})\in\mathbb{B}_n$ 可由其支撑集唯一表示，即支撑集不同，其对应的布尔函数也不同[1]。n 元布尔函数 $f_0(x_0,x_1,\cdots,x_{n-1})=\bigoplus_{i=0}^{n-1}x_i\in\mathbb{B}_n$ 是旋转对称 $(n-1)$ – 弹性函数，其中 $\mathbf{1}_{f_0}=\left\{\boldsymbol{x}\in\mathbb{F}_2^n\middle|\mathrm{wt}(\boldsymbol{x})\text{为奇数}\right\}$，$\mathbf{1}_{f_0\oplus1}=\mathbb{F}_2^n\setminus\mathbf{1}_{f_0}=\left\{\boldsymbol{x}\in\mathbb{F}_2^n\middle|\mathrm{wt}(\boldsymbol{x})\text{为偶数}\right\}$。通过改变 $f_0(\boldsymbol{x})$ 的支撑集，可以定义一个新的旋转对称布尔函数 $g(\boldsymbol{x})$，令

$$g(\boldsymbol{x})=\begin{cases}f_0(\boldsymbol{x})\oplus1, & \boldsymbol{x}\in\boldsymbol{T}\\ f_0(\boldsymbol{x}), & \boldsymbol{x}\notin\boldsymbol{T}\end{cases}\tag{2}$$

则 $\mathbf{1}_g=\mathbf{1}_{f_0}\cup\boldsymbol{T}_2\setminus\boldsymbol{T}_1$，其中，$\boldsymbol{T}=\boldsymbol{T}_1\cup\boldsymbol{T}_2\subseteq\mathbb{F}_2^n$，$\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 分别是 $\mathbf{1}_{f_0}$ 和 $\mathbf{1}_{f_0\oplus1}$ 中若干轨道的并集[24-25]。这种通过改变布尔函数的支撑集构造新函数的方法被称为交换方法。

研究 $\mathbb{F}_2^n$ 上旋转对称函数 $g(\boldsymbol{x})$ 的构造等价于研究 T 的选择，$\boldsymbol{T}=\boldsymbol{T}_1\cup\boldsymbol{T}_2$ 的选择不同，则式(2)定义的函数 $g(\boldsymbol{x})$ 也不同。本文可以通过选择合适的 T，使 $g(\boldsymbol{x})$ 具有良好的密码学性质。下面将在文献[24]的基础上进一步研究旋转对称 2–弹性函数的具体构造。

引理 2[24] 当且仅当

$$\boldsymbol{B}_{\mathbf{1}_f}=\sum_{\boldsymbol{O}_n(\boldsymbol{x})\subseteq\mathbf{1}_f}\boldsymbol{B}_{\boldsymbol{O}_n(\boldsymbol{x})}=\begin{pmatrix}2^{n-3}&2^{n-3}&2^{n-3}\\2^{n-3}&2^{n-3}&2^{n-3}\\\vdots&\vdots&\vdots\\2^{n-3}&2^{n-3}&2^{n-3}\end{pmatrix}_{\left\lfloor\frac{n}{2}\right\rfloor\times3}$$

时，$f(\boldsymbol{x})\in\mathbb{B}_n$ 是旋转对称 2–弹性函数。

引理 3[24] 假设正整数 $n\geqslant5$，向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$，当且仅当 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 的数对分布矩阵满足 $\boldsymbol{B}_{\boldsymbol{T}_1}=\boldsymbol{B}_{\boldsymbol{T}_2}$，式(2)定义的函数 $g(\boldsymbol{x})$ 是 n 元旋转对称 2–弹性函数。

由引理 2 可知，设 $g(\boldsymbol{x})$ 是旋转对称布尔函数，当且仅当

$$\boldsymbol{B}_{\mathbf{1}_g}=\boldsymbol{B}_{\mathbf{1}_{f_0}\setminus\boldsymbol{T}_1}+\boldsymbol{B}_{\boldsymbol{T}_2}=\begin{pmatrix}2^{n-3}&2^{n-3}&2^{n-3}\\2^{n-3}&2^{n-3}&2^{n-3}\\\vdots&\vdots&\vdots\\2^{n-3}&2^{n-3}&2^{n-3}\end{pmatrix}=$$

$$\boldsymbol{B}_{\mathbf{1}_{g\oplus1}}=\boldsymbol{B}_{\mathbf{1}_{f_0\oplus1}\setminus\boldsymbol{T}_2}+\boldsymbol{B}_{\boldsymbol{T}_1}$$

时，$g(\boldsymbol{x})$ 是旋转对称 2–弹性函数，即 $\boldsymbol{B}_{\boldsymbol{T}_1}=\boldsymbol{B}_{\boldsymbol{T}_2}$，其中，$\boldsymbol{T}_1\subseteq\mathbf{1}_{f_0}$ 和 $\boldsymbol{T}_2\subseteq\mathbf{1}_{f_0\oplus1}$ 都是若干轨道的并集。故当且仅当集合 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 的数对分布矩阵满足 $\boldsymbol{B}_{\boldsymbol{T}_1}=\boldsymbol{B}_{\boldsymbol{T}_2}$ 时，$f(\boldsymbol{x})$ 是 n 元旋转对称 2–弹性函数。

当 n 为奇素数时，$\mathbb{F}_2^n$ 中只有长轨道、$\mathbf{0}_n$ 和 $\mathbf{1}_n$，并且 g_n 一定是 4 的倍数。如果 $g(\boldsymbol{x})$ 是旋转对称 2–弹性函数，则根据平衡性可知，$\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 中的轨道个

表 1　　$\mathbb{F}_2^7$ 上轨道代表元及其数对分布矩阵

序号	旋转对称轨道代表元	数对分布矩阵	序号	旋转对称轨道代表元	数对分布矩阵
1	(0000000)	$\begin{pmatrix}1&0&0\\1&0&0\\1&0&0\end{pmatrix}$	11	(1111000)	$\begin{pmatrix}2&1&3\\1&2&2\\0&3&1\end{pmatrix}$
2	(1000000)	$\begin{pmatrix}5&1&0\\5&1&0\\5&1&0\end{pmatrix}$	12	(1101100)	$\begin{pmatrix}1&2&2\\0&3&1\\2&1&3\end{pmatrix}$
3	(1100000)	$\begin{pmatrix}4&1&1\\3&2&0\\3&2&0\end{pmatrix}$	13	(1101010)	$\begin{pmatrix}0&3&1\\2&1&3\\1&2&2\end{pmatrix}$
4	(1001000)	$\begin{pmatrix}3&2&0\\3&2&0\\4&1&1\end{pmatrix}$	14	(1110100)	$\begin{pmatrix}1&2&2\\1&2&2\\1&2&2\end{pmatrix}$
5	(1010000)	$\begin{pmatrix}3&2&0\\4&1&1\\3&2&0\end{pmatrix}$	15	(1110010)	$\begin{pmatrix}1&2&2\\1&2&2\\1&2&2\end{pmatrix}$
6	(1110000)	$\begin{pmatrix}3&1&2\\2&2&1\\1&3&0\end{pmatrix}$	16	(1111100)	$\begin{pmatrix}1&1&4\\0&2&3\\0&2&3\end{pmatrix}$
7	(1100100)	$\begin{pmatrix}2&2&1\\1&3&0\\3&1&2\end{pmatrix}$	17	(1110110)	$\begin{pmatrix}0&2&3\\0&2&3\\1&1&4\end{pmatrix}$
8	(1010100)	$\begin{pmatrix}1&3&0\\3&1&2\\2&2&1\end{pmatrix}$	18	(1111010)	$\begin{pmatrix}0&2&3\\1&1&4\\0&2&3\end{pmatrix}$
9	(1101000)	$\begin{pmatrix}2&2&1\\2&2&1\\2&2&1\end{pmatrix}$	19	(1111110)	$\begin{pmatrix}0&1&5\\0&1&5\\0&1&5\end{pmatrix}$
10	(1011000)	$\begin{pmatrix}2&2&1\\2&2&1\\2&2&1\end{pmatrix}$	20	(1111111)	$\begin{pmatrix}0&0&1\\0&0&1\\0&0&1\end{pmatrix}$

数一定相等，并且轨道个数一定为偶数[24]。不妨设 $\mathbf{1}_{f_0}=\boldsymbol{T}_1\cup\boldsymbol{T}_3$，$\mathbf{1}_{f_0\oplus 1}=\boldsymbol{T}_2\cup\boldsymbol{T}_4$，其中，$\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 中轨道个数为 t，$\boldsymbol{T}_3$ 和 $\boldsymbol{T}_4$ 中轨道个数为 $\frac{g_n}{2}-t$，t 和 $\frac{g_n}{2}-t$ 都是偶数[24]。当改变函数 f_0 在 $\boldsymbol{T}=\boldsymbol{T}_1\cup\boldsymbol{T}_2$ 或 $\boldsymbol{T}=\boldsymbol{T}_3\cup\boldsymbol{T}_4$ 上的函数值时，都可以得到支撑集分别为 $\boldsymbol{T}_2\cup\boldsymbol{T}_3$ 和 $\boldsymbol{T}_1\cup\boldsymbol{T}_4$ 的 2 个函数。为避免构造的函数重复，令 $2t=\min\left\{\left|\left\{\boldsymbol{O}_n(\boldsymbol{x})\,|\,\boldsymbol{O}_n(\boldsymbol{x})\subseteq\boldsymbol{T}\right\}\right|,\left|\left\{\boldsymbol{O}_n(\boldsymbol{x})\,|\,\boldsymbol{O}_n(\boldsymbol{x})\subseteq\mathbb{F}_2^n\setminus\boldsymbol{T}\right\}\right|\right\}$，即 $2\leqslant t\leqslant\frac{g_n}{4}$。

关于 n 元旋转对称 2−弹性函数的构造，本文先考虑 n 为较小的素数，显然，当 $n=3$ 或 5 时，轨道个数较少，集合 T 的可选方案也较简单。本文令 $n=7$，$t=2$ 或 4，根据 T 的可选方案具体构造了全部的旋转对称 2−弹性函数。

定理 1　在 $\mathbb{F}_2^7$ 上，有且仅有 280 个非线性旋转对称 2−弹性函数。

证明　在 $\mathbb{F}_2^7$ 上，通过选取所有满足 $\boldsymbol{B}_{\boldsymbol{T}_1}=\boldsymbol{B}_{\boldsymbol{T}_2}$ 的集合 $\boldsymbol{T}=\boldsymbol{T}_1\cup\boldsymbol{T}_2$ 的方法构造非线性旋转对称 2−弹性函数 $g(\boldsymbol{x})$，其中 $\boldsymbol{T}_1\subseteq\mathbf{1}_{f_0}$，$\boldsymbol{T}_2\subseteq\mathbf{1}_{f_0\oplus 1}$。

1) 当 $t=2$ 时，$|\boldsymbol{T}|=16$ 或 28，其中 $|\boldsymbol{T}|=28$ 不存在。$|\boldsymbol{T}|=16$ 时有 7 种方案，构造的非线性旋转对称 2−弹性函数有 2×7 个。集合 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 的选择方案如表 2 所示。

表 2 $|\boldsymbol{T}|=16$ 时集合 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 的选择方案

序号	T_1	T_2
1	(6)(20)	(1)(11)
2	(8)(20)	(1)(13)
3	(7)(20)	(1)(12)
4	(9)(20)	(1)(14)
5	(9)(20)	(1)(15)
6	(10)(20)	(1)(14)
7	(10)(20)	(1)(15)

2) 当 $t=4$ 时，$|\boldsymbol{T}|=44$ 或 56，其中 $|\boldsymbol{T}|=44$ 不存在。$|\boldsymbol{T}|=56$ 时有 133 种方案，构造的非线性旋转对称 2−弹性函数有 2×133 个。集合 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 的选择方案如表 3 所示。

所以，在 $\mathbb{F}_2^7$ 上有且仅有 2×140 个非线性旋转对称 2−弹性函数。证毕。

根据式(1)和集合 T 的选择可知

$$W_g(\boldsymbol{w})=\sum_{\boldsymbol{x}\in\mathbb{F}_2^7}(-1)^{g(\boldsymbol{x})\oplus\boldsymbol{wx}}=\sum_{\boldsymbol{x}\in\mathbb{F}_2^7\setminus\boldsymbol{T}}(-1)^{f_0(\boldsymbol{x})\oplus\boldsymbol{wx}}-\sum_{\boldsymbol{x}\in\boldsymbol{T}}(-1)^{f_0(\boldsymbol{x})\oplus\boldsymbol{wx}}=\sum_{\boldsymbol{x}\in\mathbb{F}_2^7}(-1)^{f_0(\boldsymbol{x})\oplus\boldsymbol{wx}}-2\sum_{\boldsymbol{x}\in\boldsymbol{T}}(-1)^{f_0(\boldsymbol{x})\oplus\boldsymbol{wx}}$$

其中，$|\boldsymbol{T}|=16$ 或 56。

1) 当 $\boldsymbol{w}=\mathbf{1}_7$ 时，$W_g(\boldsymbol{w})=2^7-2\sum_{\boldsymbol{x}\in\mathrm{T}}(-1)^{f_0(\boldsymbol{x})\oplus\boldsymbol{wx}}=2^7-2|\boldsymbol{T}|$。

2) 当 $\boldsymbol{w}\neq\mathbf{1}_7$ 时，$\left|W_g(\boldsymbol{w})\right|=\left|2\sum_{\boldsymbol{x}\in\boldsymbol{T}}(-1)^{f_0(\boldsymbol{x})\oplus\boldsymbol{wx}}\right|\leqslant 2|\boldsymbol{T}|$。

根据文献[10]可知，7 元旋转对称 2−弹性函数的非线性度不超过 56。若 $2^7-2|\boldsymbol{T}|\geqslant 2|\boldsymbol{T}|$，则 $|\boldsymbol{T}|\leqslant 32$，所以，关于所构造函数的非线性度有 2 种情况。

1) 当 $|\boldsymbol{T}|=16$ 时，所构造的旋转对称 2−弹性函数都在 $\boldsymbol{w}=\mathbf{1}_7$ 处取得最大 Walsh 值，即

$$NL(g)=2^6-\frac{1}{2}\max_{\boldsymbol{w}\in\mathbb{F}_2^n}\left|W_g(\boldsymbol{w})\right|=16$$

2) 当 $|\boldsymbol{T}|=56$ 时，存在非线性度为 56 的函数。在表 3 中，通过计算机程序搜索，根据序号为 9、10、13、16、18、19、24、27、30、31、45、46、49、50、55、56、58、59、63、66、69、70、79、82、83、86、89、90、100、101、103、104、107、108、124、125 的 T 的选择方案所构造的 2×36 个旋转对称 2−弹性函数是非线性度 56 的最优函数。

推论 1 当 k 为奇数时，$\mathbb{F}_2^{7k}$ 上的非线性旋转对称 2−弹性函数至少有 280 个。

证明 由引理 3 可知，当且仅当 $\boldsymbol{B}_{\boldsymbol{T}_1}=\boldsymbol{B}_{\boldsymbol{T}_2}$ 时，支撑集为 $\mathbf{1}_g=\mathbf{1}_{f_0}\cup\boldsymbol{T}_2\setminus\boldsymbol{T}_1$ 的旋转对称函数 $g(\boldsymbol{x})$ 是 2−弹性的，即矩阵 $\boldsymbol{T}_1$ 的任意两列中数对 00、01(10)、11 出现的频次与矩阵 $\boldsymbol{T}_2$ 中相同位置的两列中数对出现的频次相等。

不妨设 $\boldsymbol{T}_1=\bigcup_{i=1}^{t}\boldsymbol{O}_7(\boldsymbol{\alpha}_i)$，$\boldsymbol{T}_2=\bigcup_{j=1}^{t}\boldsymbol{O}_7(\boldsymbol{\beta}_j)$，其中 $\boldsymbol{\alpha}_i,\boldsymbol{\beta}_j\in\mathbb{F}_2^7$，$i,j$ 为正整数，$t=2$ 或 4。当 $n=7k$ 且 k 为奇数时，$\mathbf{1}_k\otimes\boldsymbol{\alpha}_i\in\mathbb{F}_2^n$ 和 $\mathbf{1}_k\otimes\boldsymbol{\beta}_j\in\mathbb{F}_2^n$ 分别满足 $\mathrm{wt}(\mathbf{1}_k\otimes\boldsymbol{\alpha}_i)$ 为奇数，$\mathrm{wt}(\mathbf{1}_k\otimes\boldsymbol{\beta}_j)$ 为偶数。进一步地，令 $\boldsymbol{T}_1'=\bigcup_{i=1}^{t}\boldsymbol{O}_{7k}(\mathbf{1}_k\otimes\boldsymbol{\alpha}_i)\subseteq\mathbf{1}_{f_0}$，$\boldsymbol{T}_2'=\bigcup_{j=1}^{t}\boldsymbol{O}_{7k}(\mathbf{1}_k\otimes\boldsymbol{\beta}_i)\subseteq\mathbf{1}_{f_0\oplus 1}$，这里 $f_0\in\mathbb{B}_{7k}$，则根据 $\boldsymbol{B}_{\boldsymbol{T}_1}=\boldsymbol{B}_{\boldsymbol{T}_2}$ 可知，矩阵 $\boldsymbol{T}_1'$ 的任意两列中数对 00、01(10)、11 出现的频次与矩阵 $\boldsymbol{T}_2'$ 中相同位置的两列中数对出现的频次相等，即 $\boldsymbol{B}_{\boldsymbol{T}_1'}=\boldsymbol{B}_{\boldsymbol{T}_2'}$。所以，如果有 $\boldsymbol{T}=\boldsymbol{T}_1\cup\boldsymbol{T}_2$ 使 7 元旋转对称 2−弹性函数存在，那么就有 $\boldsymbol{T}'=\boldsymbol{T}_1'\cup\boldsymbol{T}_2'$ 使 $7k$ 元的旋转对称 2−弹性函数存在，也就是说 $\mathbb{F}_2^{7k}$ 上至少存在 280 个非线性旋转对称 2−弹性函数。证毕。

3 结束语

旋转对称布尔函数因其特殊的结构和性质而受到广泛关注，关于旋转对称弹性函数的研究也越来越多。旋转对称 1−弹性函数的构造与计数已基本被解决，但是关于旋转对称 2−弹性函数还有许多开放性的问题。本文基于数对分布矩阵的性质，通过修改线性函数 $f(x_0,x_1,\cdots,x_{n-1})=x_0\oplus x_1\oplus\cdots\oplus x_{n-1}$ 的支撑集，彻底解决了 $\mathbb{F}_2^7$ 上旋转对称 2−弹性函数的构造问题。当 n 是大于 7 的奇数时，如果旋转对称轨道 $O_n(\boldsymbol{x})$ 满足 $\mathrm{wt}(\boldsymbol{x})$ 为奇数，那么轨道 $O_n(\bar{\boldsymbol{x}})$ 满足 $\mathrm{wt}(\bar{\boldsymbol{x}})$ 是偶数，并且轨道 $O_n(\boldsymbol{x})$ 与轨道 $O_n(\bar{\boldsymbol{x}})$ 的数对分布矩阵之间存在特殊的数量关系。下一步，笔者将从向量互补的旋转对称轨道着手，选取满足 $B_{T_1}=B_{T_2}$ 的 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$，构造一类奇数变元的旋转对称 2−弹性函数。更一般的构造也是笔者未来会一直关注的问题。

表 3　　$|T|=56$ 时 T_1 和 T_2 的选择方案

序号	T_1	T_2	序号	T_1	T_2	序号	T_1	T_2
1	(6)(16)(17)(18)	(11)(14)(15)(198)	46	(7)(8)(9)(16)	(5)(12)(14)(15)	91	(7)(8)(9)(17)	(4)(12)(13)(14)
2	(7)(6)17)(18)	(12)(14)(15)(19)	47	(7)(8)(10)(16)	(3)(12)(13)(14)	92	(7)(8)(9)(17)	(4)(12)(13)(15)
3	(8)(16)(17)(18)	(13)(14)(15)19)	48	(7)(8)(10)(16)	(3)(12)(13)(15)	93	(7)(8)(10)(17)	(4)(12)(13)(14)
4	(9)(16)(17)(18)	(11)(12)(13)(19)	49	(7)(8)(10)(16)	(4)(11)(12)(13)	94	(7)(8)(10)(17)	(4)(12)(13)(15)
5	(10)(16)(17)(18)	(11)(12)(13)(19)	50	(7)(8)(10)(16)	(5)(12)(14)(15)	95	(7)(9)(10)(17)	(4)(12)(14)(15)
6	(2)(6)(6)(17)	(3)(4)(11)(9)	51	(7)(9)(10)(16)	(3)(12)(14)(15)	96	(8)(9)(10)(17)	(4)(13)(14)(15)
7	(2)(7)(16)(17)	(3)(4)(12)(19)	52	(7)(9)(10)(16)	(4)(11)(12)(14)	97	(8)(9)(10)(17)	(5)(12)(13)(14)
8	(2)(8)(16)(17)	(3)(4)(13)(19)	53	(7)(9)(10)(16)	(4)(11)(12)(15)	98	(8)(9)(10)(17)	(5)(12)(13)(15)
9	(2)(8)(16)(17)	(4)(5)(14)(19)	54	(8)(9)(10)(16)	(3)(13)(14)(15)	99	(6)(7)(8)(18)	(3)(13)(14)(15)
10	(2)(8)(16)(17)	(4)(5)(15)(19)	55	(8)(9)(10)(16)	(4)(11)(13)(14)	100	(6)(7)(8)(18)	(4)(11)(13)(14)
11	(2)(9)(16)(17)	(3)(4)(14)(19)	56	(8)(9)(10)(16)	(4)(11)(13)(15)	101	(6)(7)(8)(18)	(4)(11)(13)(15)
12	(2)(9)(16)(17)	(3)(4)(15)19)	57	(8)(9)(10)(16)	(5)(11)(12)(13)	102	(6)(7)(8)(18)	(5)(11)(12)(13)
13	(2)(9)(16)(17)	(3)(5)(12)(19)	58	(2)(6)(17)(18)	(3)(5)(14)(19)	103	(6)(7)(9)(18)	(3)(11)(12)(13)
14	(2)(10)(16)(17)	(3)(4)(14)(19)	59	(2)(6)(17)(18)	(3)(5)(15)(19)	104	(6)(7)(9)(18)	(4)(11)(14)(15)
15	(2)(10)(16)(17)	(3)(4)(15)19)	60	(2)(6)(17)(18)	(4)(5)(11)(19)	105	(6)(7)(9)(18)	(5)(11)(12)(14)
16	(2)(10)(16)(17)	(3)(5)(12)(19)	61	(2)(7)(17)(18)	(4)(5)(12)(19)	106	(6)(7)(9)(18)	(5)(11)(12)(15)
17	(2)(6)(16)(18)	(3)(5)(11)(19)	62	(2)(8)(17)(18)	(4)(5)(13)(19)	107	(6)(7)(10)(18)	(3)(11)(12)(13)
18	(2)(7)(16)(18)	(3)(4)(14)19)	63	(2)(9)(17)(18)	(3)(4)(13)(19)	108	(6)(7)(10)(18)	(4)(11)(14)(15)
19	(2)(7)(16)(18)	(3)(4)(15)(19)	64	(2)(9)(17)(18)	(4)(5)(14)(19)	109	(6)(7)(10)(18)	(5)(11)(12)(14)
20	(2)(7)(16)(18)	(3)(5)(12)(19)	65	(2)(9)(17)(18)	(4)(5)(15)(19)	110	(6)(7)(10)(18)	(5)(11)(12)(15)
21	(2)(8)(16)(18)	(3)(5)(13)(19)	66	(2)10)(17)(18)	(3)(4)(13)(19)	111	(6)(8)(9)(18)	(5)(11)(13)(14)
22	(2)(9)(16)(18)	(3)(5)(14)(19)	67	(2)(10)(17)(18)	(4)(5)(14)(19)	112	(6)(8)(9)(18)	(5)(11)(13)(15)
23	(2)(9)(16)(18)	(3)(5)(15)(19)	68	(2)(10)(17)(18)	(4)(5)(15)(19)	113	(6)(8)(10)(18)	(5)(11)(13)(14)
24	(2)(9)(16)(18)	(4)(5)(11)(19)	69	(6)(7)(8)(17)	(3)(12)(13)(14)	114	(6)(8)(10)(18)	(5)(11)(13)(15)
25	(2)(10)(16)(18)	(3)(5)(14)(19)	70	(6)(7)(8)(17)	(3)(12)(13)(15)	115	(6)(8)(10)(18)	(3)(11)(13)(14)
26	(2)(10)(16)(18)	(3)(5)(15)(19)	71	(6)(7)(8)(17)	(4)(11)(12)(13)	116	(6)(9)(10)(18)	(3)(11)(13)(15)
27	(2)(10)(16)(18)	(4)(5)(11)(19)	72	(6)(7)(8)(17)	(5)(12)(14)(15)	117	(6)(9)(10)(18)	(5)(11)(14)(15)
28	(6)(7)(8)(16)	(3)(11)(12)(13)	73	(6)(7)(9)(17)	(3)(12)(14)(15)	118	(7)(8)(9)(18)	(4)(13)(14)(15)
29	(6)(7)(8)(16)	(4)(11)(14)(15)	74	(6)(7)(9)(17)	(4)(11)(12)(14)	119	(7)(8)(9)(18)	(5)(12)(13)(14)
30	(6)(7)(8)(6)	(5)(11)(12)(14)	75	(6)(7)(9)(17)	(4)(11)(12)(15)	120	(7)(8)(9)(18)	(5)(12)(13)(15)
31	(6)(7)(8)(16)	(5)(11)(12)(15)	76	(6)(7)(10)(17)	(3)(12)(14)(15)	121	(7)(8)(10)(18)	(4)(13)(14)(15)
32	(6)(7)(9)(16)	(3)(11)(12)(14)	77	(6)(7)(10)(17)	(4)(11)(12)(14)	122	(7)(8)(10)(18)	(5)(12)(13)(14)
33	(6)(7)(9)(6)	(3)(11)(12)(15)	78	(6)(7)(10)(17)	(4)(11)(12)(15)	123	(7)(8)(10)(18)	(5)(12)(13)(15)
34	(6)(7)(10)(16)	(3)(11)(12)(14)	79	(6)(8)(9)(17)	(3)(13)(14)(15)	124	(7)(8)(10)(18)	(3)(12)(13)(14)
35	(6)(7)(10)(16)	(3)(11)(12)(15)	80	(6)(8)(9)(17)	(4)(11)(13)(14)	125	(7)(9)(10)(18)	(3)(12)(13)(15)
36	(6)(8)(9)(16)	(3)(11)(13)(14)	81	(6)(8)(9)(17)	(4)(11)(13)(15)	126	(7)(9)(10)(18)	(4)(11)(12)(13)
37	(6)(8)(9)(16)	(3)(11)(13)(15)	82	(6)(8)(9)(17)	(5)(11)(12)(13)	127	(7)(9)(10)(18)	(5)(12)(14)(15)
38	(6)(8)(9)(16)	(5)(11)(14)(15)	83	(6)(8)(10)(17)	(3)(13)(14)(15)	128	(8)(9)(10)(18)	(5)(13)(14)(15)
39	(6)(8)(10)(6)	(3)(11)(13)(14)	84	(6)(8)(10)(17)	(4)(11)(13)(14)	129	(2)(6)(7)(8)	(3)(4)(5)(14)
40	(6)(8)(10)(16)	(3)(11)(13)(15)	85	(6)(8)(10)(17)	(4)(11)(13)(15)	130	(2)(6)(7)(8)	(3)(4)(5)(15)
41	(6)(8)10)(16)	(5)(11)(14)(15)	86	(6)(8)(10)(17)	(5)(11)(12)(13)	131	(2)(6)(9)(10)	(3)(4)(5)(11)
42	(6)(9)(10)(6)	(3)(11)(14)(15)	87	(6)(9)(10)(17)	(3)(11)(12)(13)	132	(2)(7)(9)(10)	(3)(4)(5)(12)
43	(7)(8)(9)(16)	(3)(12)(13)(l4)	88	(6)(8)(10)(17)	(4)(11)(14)(15)	133	(2)(8)(9)(10)	(3)(4)(5)(13)
44	(7)(8)(9)(16)	(3)(12)(13)(15)	89	(6)(9)(10)(17)	(5)(11)(12)(14)			
45	(7)(8)(9)(16)	(4)(11)(12)(13)	90	(6)(9)(10)(17)	(5)(11)(12)(15)			

参考文献：

[1] 李超, 屈龙江, 周悦. 密码函数的安全性指标分析[M]. 北京: 科学出版社, 2011.
LI C, QU L J, ZHOU Y. Security index analysis of cryptographic functions[M]. Beijing: Science Press, 2011.

[2] ZHANG W Y. Construction of balanced rotation symmetric Boolean functions with optimal algebraic immunity[J]. Wuhan University Journal of Natural Sciences, 2014, 19(4): 301-306.

[3] FU S, LI C, MATSUURA K, et al. Balanced 2p-variable rotation symmetric Boolean functions with maximum algebraic immunity[J]. Applied Mathematics Letters, 2011, 24(12): 2093-2096.

[4] SUN L, SHI Z X. Balanced rotation symmetric Boolean functions with good autocorrelation properties[J]. IEEE Access, 2021, 9: 67850-67858.

[5] FU S J, LI C, QU L J. On the number of rotation symmetric Boolean functions[J]. Science China Information Sciences, 2010, 53(3): 537-545.

[6] STANICA P, MAITRA S, CLARK J A. Results on rotation symmetric bent and correlation immune Boolean functions[C]//International Workshop on Fast Software Encryption. Berlin: Springer, 2004: 161-177.

[7] STANICA P, MAITRA S. Rotation symmetric Boolean functions—count and cryptographic properties[J]. Discrete Applied Mathematics, 2008, 156(10):1567-1580.

[8] PIEPRZYK J, QU C X. Fast hashing and rotation-symmetric functions[J]. Journal of Universal Computer Science, 1999, 5(1): 20-31.

[9] KAVUT S, MAITRA S, SARKAR S, et al. Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity>240[C]//International Conference on Cryptology. Berlin: Springer, 2006: 266-279.

[10] KAVUT S, MAITRA S, YUCEL M D. Search for Boolean functions with excellent profiles in the rotation symmetric class[J]. IEEE Transactions on Information Theory, 2007, 53(5): 1743-1751.

[11] CARLET C, DALAI D K, GUPTA K C, et al. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction[J]. IEEE Transactions on Information Theory, 2006, 52(7): 3105-3121.

[12] 高光普, 程庆丰, 王磊. 三次旋转对称 Bent 函数的构造[J]. 密码学报, 2015, 2(4): 372-380.
GAO G P, CHENG Q F, WANG L. Construction of cubic rotation symmetric Bent functions[J]. Journal of Cryptologic Research, 2015, 2(4): 372-380.

[13] ZHANG W Y, HAN G Y. Construction of rotation symmetric Bent functions with maximum algebraic degree[J]. Science China Information Sciences, 2018, 61(3): 1-3.

[14] 郑东, 严宏超, 赵庆兰. 一类旋转对称 Bent 函数的构造[J]. 西安邮电大学学报, 2018, 23(2): 17-21.
ZHENG D, YAN H C, ZHAO Q L. Construction of a class of rotation symmetric Bent functions[J]. Journal of Xi'an University of Posts and Telecommunications, 2018, 23(2): 17-21.

[15] SU S H. Systematic methods of constructing Bent functions and 2-rotation symmetric Bent functions[J]. IEEE Transactions on Information Theory, 2020, 66(5): 3277-3291.

[16] 李超, 薛朝红, 付绍静. 代数免疫度最优的旋转对称布尔函数的构造[J]. 国防科技大学学报, 2012, 34(2): 34-38.
LI C, XUE C H, FU S J. Construction of rotation symmetric Boolean function with maximum algebraic immunity[J]. Journal of National University of Defense Technology, 2012, 34(2): 34-38.

[17] 张鹏, 付绍静, 屈龙江, 等. 平衡旋转对称布尔函数的计数[J]. 应用科学学报, 2012, 30(1): 45-51.
ZHANG P, FU S J, QU L J, et al. Enumeration of balanced rotation-symmetric Boolean functions[J]. Journal of Applied Sciences, 2012, 30(1): 45-51.

[18] 杜蛟, 温巧燕, 张劼, 等. 2p 元 2-阶旋转对称弹性布尔函数的构造与计数[J]. 北京邮电大学学报, 2012, 35(5): 36-40.
DU J, WEN Q Y, ZHANG J, et al. Construction and counting of resilient 2-rotation symmetric Boolean functions with 2p variables[J]. Journal of Beijing University of Posts and Telecommunications, 2012, 35(5): 36-40.

[19] PANG S Q, WANG X N, WANG J, et al. Construction and count of 1-resilient rotation symmetric Boolean functions[J]. Information Sciences, 2018, 450: 336-342.

[20] DU J, WEN Q Y, ZHANG J, et al. Constructions of resilient rotation symmetric Boolean functions on given number of variables[J]. IET Information Security, 2014, 8(5):265-272.

[21] SUN L, FU F W, GUANG X. Two classes of 1-resilient prime-variable rotation symmetric Boolean functions[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, 100(3): 902-907.

[22] SUN L, SHI Z X, FU F W. Several classes of even-variable 1-resilient rotation symmetric Boolean functions with high algebraic degree and nonlinearity[J]. Discrete Mathematics, 2022, 345(3):112752.

[23] 杜蛟, 刘春红, 庞善起. 4t−1 元旋转对称 2-弹性函数的构造[J]. 通信学报, 2020, 41(11): 169-175.
DU J, LIU C H, PANG S Q. Constructions of rotation symmetric 2-resilient functions with 4t−1 number of variables[J]. Journal on Communications, 2020, 41(11): 169-175.

[24] DU J, CHEN Z Y, DONG L, et al. A new characterization of 2-resilient rotation symmetric Boolean functions[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2023, 106 (9):1268-1271.

[25] DU J, CHEN Z Y, FU S J, et al. Constructions of 2-resilient rotation symmetric Boolean functions through symbol transformations of cyclic Hadamard matrix[J]. Theoretical Computer Science, 2022, 919: 80-91.

[作者简介]

杜蛟（1978− ），男，湖北英山人，博士，河南师范大学副教授、硕士生导师，主要研究方向为现代密码学中的布尔函数与序列设计、编码密码的数学理论。

李琳（1998− ），女，河南信阳人，河南师范大学硕士生，主要研究方向为编码密码的数学理论。

赵紫薇（1999− ），女，河南周口人，河南师范大学硕士生，主要研究方向为编码密码的数学理论。

李月月（1990− ），女，河南安阳人，博士，河南师范大学讲师、硕士生导师，主要研究方向为仿射代数几何、编码密码的数学理论。

王天银（1979− ），男，河南南阳人，博士，洛阳师范学院教授、硕士生导师，主要研究方向为密码学、隐私保护。