旋转对称3-弹性函数的等价刻画

张慧[1]，陈晓婷[1]，王宏盼[1]，杜蛟[1]，李功丽[2]，王天银[1,3]
（1.河南师范大学数学与统计学院（密码学院），河南 新乡 453007；2.河南师范大学计算机与信息工程学院，河南 新乡 453007；
3.洛阳师范学院通信工程学院，河南 洛阳 471934）

摘要：旋转对称布尔函数凭借优良的密码学特性，在分组密码S盒与Hash函数的设计中得到广泛应用，是对称密码领域的研究热点。基于此，建立了旋转对称3-弹性函数的两类等价刻画形式。通过定义旋转对称轨道的3-重分布矩阵，推导出旋转对称函数满足3-弹性性质的充要条件。结合弹性函数与正交表的关系，将旋转对称3-弹性函数的构造问题转化为特定方程组的求解问题。

关键词：旋转对称函数；3-重分布矩阵；正交表；弹性函数；方程组
中图分类号：TN918.1
文献标志码：A
doi：10.11959/j.issn.1000–436x.TXXB260091

Characterization of 3-resilient rotation symmetric functions

Zhang Hui[1], Chen Xiaoting[1], Wang Hongpan[1], Du Jiao[1], Li Gongli[2], Wang Tianyin[1,3]
1. School of Mathematics and Statistics (School of Cryptography), Henan Normal University, Xinxiang 453007, China
2. College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China
3. School of Communication Engineering, Luoyang Normal University, Luoyang 471934, China

Abstract: Rotation symmetric Boolean function (RSBF) is widely employed in the design of block cipher S-boxes and hash functions due to their strong cryptographic characteristics. Based on this, two types of equivalent characterizations for rotation symmetric 3-resilient functions were established. By defining the concept of the 3-tuples distribution matrix of rotation symmetric orbits, the necessary and sufficient conditions for a rotation symmetric function were deduced to satisfy the 3-resilience property. Furthermore, combining the intrinsic relations between resilient functions and orthogonal arrays, it is shown that the constructions of 3-resilient RSBF are equivalent to solve a system of equations.

Key words: rotation symmetric function, 3-tuples distribution matrix, orthogonal array, resilient function, system of equation

0 引言

Shannon[1]提出的扩散与混淆的经典思想已发展成对称密码设计领域的通用准则。为实现高效的混淆与扩散效果，抵御最佳仿射逼近攻击[2]、线性攻击[3]、相关攻击[4]及差分攻击[5]等各类常见的密码攻击手段，密码学研究中使用的布尔函数需满足相应的安全性指标，包括平衡性、代数免疫度、代数次数、非线性度、相关免疫度、差分均匀度和严格雪崩准则等。然而，这些安全性指标之间存在相互约束的关系，因此，如何设计出能够同时满足多项安全性指标的布尔函数，

收稿日期：2026–02–08；**修回日期：**2026–04–10
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.62572221, No.62272208）；国家重点研发计划基金资助项目（No.2024YFA1013000）；河南省自然科学基金资助项目（No.252300421872）；中国博士后科学基金资助项目（No.GZC20252042）
Foundation Items: The National Natural Science Foundation of China (No.62372157, No.62572221, No.62272208), The National Key Research and Development Program of China (No. 2024YFA1013000), Henan Provincial Natural Science Foundation (No.252300421872), The China Postdoctoral Science Foundation (No.GZC20252042)

始终是密码学领域中亟待深入探索的一个重要课题。

1998 年，Filliol 和 Fontaine[6]在 Eurocrypt 会议上首次提出旋转对称布尔函数，该类函数具有结构简单、存储需求低和运算效率高等优点。1999 年，Pieprzyk 和 Qu[7]对该类函数在哈希算法轮函数中的应用展开了系统性研究。截至目前，旋转对称布尔函数已成功应用于信息摘要算法 4（message-digest algorithm 4，MD4）、信息摘要算法 5（message-digest algorithm 5，MD5）和可变长度哈希算法（Hash of variable length，HAVAL）等 Hash 算法[7]设计中，同时在组合设计、序列设计等相关领域也彰显出重要的应用价值[8-9]。在理论研究层面，国内外研究者围绕旋转对称布尔函数展开了深入的研究，内容涵盖旋转对称轨道个数分析[10-11]、具有最优代数免疫度的旋转对称布尔函数构造[12-13]、旋转对称 bent 函数构造[14-15]以及旋转对称弹性函数构造[16-18]等多个方向。

1984 年，Siegenthaler[19]首次提出 m 阶相关免疫函数的概念，并推导出该类函数的一个充分性判定条件。1985 年，Chor 等[20]在计算机科学基础研讨会上进一步提出弹性函数的概念。1993 年，Stinson[21]揭示了弹性函数与正交表大集之间的内在关系。2014 年，Du 等[16]基于这一关联，将弹性函数的构造问题转化为方程组的求解问题。在此基础上，Du 和 Sun 等[16-18,22-23]针对有限域上任意元旋转对称 1-弹性和 2-弹性函数构造和计数问题开展了深入研究。2019 年，Sun 等[22]基于 Maiorana-McFarland 函数的二级构造框架，提出了一类 $2m$ ($m \geqslant 5$) 元旋转对称 1-弹性函数，该类函数的代数次数可达 $2m-2$，非线性度下界为 $2^{2m-1}-2^m-4m+8$。2022 年，Du 等[18,23]基于循环 Hadamard 矩阵的性质，成功构造出具有较高非线性度的旋转对称 2-弹性函数。2024 年，Du 等[17,24]通过引入数对分布矩阵这一关键研究工具，构造出若干新的旋转对称 2-弹性函数。

本文研究了两类旋转对称 3-弹性函数的刻画。首先，通过引入旋转对称轨道的 3-重分布矩阵，推导出构造一类旋转对称 3-弹性函数的充要条件；其次，结合弹性函数与正交表之间的联系，将旋转对称 3-弹性函数的构造问题转化为特定代数方程组的求解问题。

1 预备知识

设 $\boldsymbol{F}_2^n$ 为有限域 $\boldsymbol{F}_2$ 上的 n 维向量空间，映射 f: $\boldsymbol{F}_2^n \to \boldsymbol{F}_2$ 为 n 元布尔函数。记 B_n 为 $\boldsymbol{F}_2^n$ 上全体 n 元布尔函数构成的集合，+和 $\oplus$ 分别表示实数域和有限域 $\boldsymbol{F}_2$ 上的求和运算。设 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\boldsymbol{F}_2^n$，定义 $\boldsymbol{x}$ 的共轭为 $\bar{\boldsymbol{x}}=(x_1\oplus 1,x_2\oplus 1,\cdots,x_n\oplus 1)\in\boldsymbol{F}_2^n$，$\boldsymbol{x}$ 的支撑集为 $\mathrm{supp}(\boldsymbol{x})=\{i|x_i=1,1\leqslant i\leqslant n\}$，集合 $\mathrm{supp}(\boldsymbol{x})$ 中所含元素的个数称为向量 $\boldsymbol{x}$ 的汉明重量，记 $f(\boldsymbol{x})$ 的支撑集为 $\mathrm{supp}(f)=\{\boldsymbol{x}|f(\boldsymbol{x})=1,\boldsymbol{x}\in\boldsymbol{F}_2^n\}$，如果将 $\boldsymbol{F}_2^n$ 中所有向量 $\boldsymbol{x}\in\boldsymbol{F}_2^n$ 按字典序从小到大排列，则布尔函数 f 的真值表为：

$$(f(0,\cdots,0,0),f(0,\cdots,0,1),\cdots,f(1,\cdots,1,1)) \tag{1}$$

每一个布尔函数都可以被它的真值表唯一表示。对于任意 $f\in B_n$，f 的真值表中所含 1 的个数称为 f 的汉明重量，记为 $\mathrm{wt}(f)$ 或者 $|\mathrm{supp}(f)|$。若 $\mathrm{wt}(f)=|\mathrm{supp}(f)|=2^{n-1}$，则称函数 f 是平衡的。将矩阵 $\boldsymbol{A}=(a_{ij})_{n\times m}$ 和 $\boldsymbol{B}=(b_{ij})_{n\times m}$ 的 Kronecker 积记作 $\boldsymbol{A}\otimes\boldsymbol{B}$，用 $\boldsymbol{A}^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{A}$ 的转置，$\boldsymbol{0}_s$ 和 $\boldsymbol{1}_s$ 分别表示元素全为 0 和 1 的 $1\times s$ 行向量。

给定一个函数 $f\in B_n$，若它的支撑集 $\mathrm{supp}(f)$ 中有 w 个向量 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_w$，将这 w 个向量作为行向量，若不引起混淆，则 f 的支撑集也可以表示为如下支撑矩阵的形式[16]：

$$\mathrm{supp}(f)=\begin{pmatrix}\boldsymbol{a}_1\\ \boldsymbol{a}_2\\ \vdots\\ \boldsymbol{a}_w\end{pmatrix}=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\ a_{21}&a_{22}&\cdots&a_{2n}\\ \vdots&\vdots&&\vdots\\ a_{w1}&a_{w2}&\cdots&a_{wn}\end{pmatrix} \tag{2}$$

设向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\boldsymbol{F}_2^n$，对于任意的 $0\leqslant l\leqslant n-1$，定义：

$$\rho_n^l(x_1,x_2,\cdots,x_n)=(\rho_n^l(x_1),\rho_n^l(x_2),\cdots,\rho_n^l(x_n)) \tag{3}$$

其中，$\rho_n^l(x_i)=x_{i+l(\mathrm{mod}\,n)}$[7]。

定义 1 [7] 设 f 是 $\boldsymbol{F}_2^n$ 上的 n 元布尔函数，若对于任意的 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\boldsymbol{F}_2^n$，都满足 $f(\rho_n^l(x_1,x_2,\cdots,x_n))=f(x_1,x_2,\cdots,x_n)$，其中 $0\leqslant l\leqslant n-1$，则 f 是旋转对称布尔函数。

定义 2[16,21] 设 $\boldsymbol{A}$ 是一个 $\boldsymbol{F}_2$ 上的 $\omega\times n$ 矩阵，若 $\boldsymbol{A}$ 的任意 d 列组成的子矩阵的行向量中，$\boldsymbol{F}_2^d$ 中的每一个向量都出现相同次数，则称 $\boldsymbol{A}$ 是 2 水平、强度 d 的正交表，记为 $\mathbf{OA}(w,n,2,d)$。

定义 3[21,25]　假设函数 $f \in B_n$，则 f 被称为 d 阶相关免疫函数（d-correlation immune function，d-CI）当且仅当其支撑矩阵是一个正交表 $\mathbf{OA}\left(\left|\mathrm{supp}\left(f\right)\right|,n,2,d\right)$。特别地，如果 $\left|\mathrm{supp}\left(f\right)\right| = 2^{n-1}$ 成立，则 f 为 d 阶弹性函数。

引理 1[26]　$f \in B_n$ 是 t 阶相关免疫函数，当且仅当对于 $\boldsymbol{F}_2^n$ 中满足 $1 \leqslant \mathrm{wt}(\boldsymbol{\alpha}) \leqslant t$ 的 $\boldsymbol{\alpha}$，都有 $S_f(\boldsymbol{\alpha}) = 0$，其中 $S_f(\boldsymbol{\alpha}) = \sum\limits_{\boldsymbol{x} \in \boldsymbol{F}_2^n} f(\boldsymbol{x})(-1)^{\boldsymbol{\alpha} \cdot \boldsymbol{x}}$ 是 f 在点 $\boldsymbol{\alpha}$ 处的傅里叶（Fourier）变换。

借助关系 $(-1)^{f(\boldsymbol{x})} = 1 - 2f(\boldsymbol{x})$，可得到 $S_f(\boldsymbol{\alpha})$ 与 $W_f(\boldsymbol{\alpha})$ 的关系为：

$$W_f(\boldsymbol{\alpha}) = \begin{cases} -2S_f(\boldsymbol{\alpha}), \boldsymbol{\alpha} \neq 0 \\ 2^n - 2S_f(\boldsymbol{\alpha}), \boldsymbol{\alpha} = 0 \end{cases} \tag{4}$$

2　n 元 3-弹性旋转对称布尔函数的刻画

本文通过两种方法给出旋转对称 3-弹性函数的等价刻画。首先，定义旋转对称轨道的 3-重分布矩阵，推导其与 3-弹性性质的充要关系；然后，基于弹性函数与正交表的关系，将构造问题转化为方程组求解。

2.1　3-重分布矩阵

任取 $\boldsymbol{x} = \left(x_1, x_2, \cdots, x_n\right) \in \boldsymbol{F}_2^n$ 且 $\mathrm{wt}(\boldsymbol{x}) = \omega$，若 $|\boldsymbol{O}_n(\boldsymbol{x})| = l$ 且满足 $n = s \times l$，则其轨道矩阵[17,24]表示为：

$$\boldsymbol{O}_n(\boldsymbol{x}) = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_2 & x_3 & \cdots & x_1 \\ \vdots & \vdots & & \vdots \\ x_l & x_{l+1} & \cdots & x_{l-1} \end{pmatrix} = \left(\boldsymbol{X}_1, \boldsymbol{X}_2, \cdots, \boldsymbol{X}_n\right) = \mathbf{1}_s \otimes \left(\boldsymbol{X}_1, \boldsymbol{X}_2, \cdots, \boldsymbol{X}_l\right) \tag{5}$$

其中，$\boldsymbol{X}_i$ 表示矩阵 $\boldsymbol{O}_n(\boldsymbol{x})$ 的第 i 列。在子矩阵 $\left(\boldsymbol{X}_i, \boldsymbol{X}_j, \boldsymbol{X}_t\right)$ 的行向量中，记 3-重 $(0,0,0)$、$(0,0,1)$、$(0,1,0)$、$(0,1,1)$、$(1,0,0)$、$(1,0,1)$、$(1,1,0)$、$(1,1,1)$ 出现的频次分别为 N_0、N_1、N_2、N_3、N_4、N_5、N_6、N_7，称 $(N_0, N_1, N_2, N_3, N_4, N_5, N_6, N_7)$ 为子矩阵 $\left(\boldsymbol{X}_i, \boldsymbol{X}_j, \boldsymbol{X}_t\right)$ 的 3-重分布。如果一个矩阵的每一行都是某一个子矩阵 $\left(\boldsymbol{X}_i, \boldsymbol{X}_j, \boldsymbol{X}_t\right)$ 的 3-重分布，具有最少的行数，则该矩阵被称为轨道 $\boldsymbol{O}_n(\boldsymbol{x})$ 的 3-重分布矩阵，其中 $1 \leqslant i < j < t \leqslant n$，则有：

$$\begin{cases} N_0 + N_1 + N_2 + N_3 = l - \dfrac{\omega}{s} \\ N_0 + N_4 + N_2 + N_6 = l - \dfrac{\omega}{s} \\ N_0 + N_4 + N_1 + N_5 = l - \dfrac{\omega}{s} \\ N_4 + N_5 + N_6 + N_7 = \dfrac{\omega}{s} \\ N_1 + N_5 + N_3 + N_7 = \dfrac{\omega}{s} \\ N_2 + N_6 + N_3 + N_7 = \dfrac{\omega}{s} \end{cases} \tag{6}$$

进一步得到：

$$\begin{cases} N_4 + N_6 = N_1 + N_3 \\ N_4 + N_5 = N_2 + N_3 \\ N_1 + N_5 = N_2 + N_6 \end{cases} \tag{7}$$

且有：

$$N_7 + N_5 - N_2 - N_0 = \frac{2\omega}{s} - l \tag{8}$$

定理 1　令 $n \geqslant 4$，假设 $\boldsymbol{x} \in \boldsymbol{F}_2^n$ 满足 $|\boldsymbol{O}_n(\boldsymbol{x})| = n$，3-重 $(0,0,0)$、$(0,0,1)$、$(0,1,0)$、$(0,1,1)$、$(1,0,0)$、$(1,0,1)$、$(1,1,0)$、$(1,1,1)$ 在 $\boldsymbol{O}_n(\boldsymbol{x}) = \left(\boldsymbol{X}_1, \boldsymbol{X}_2, \cdots, \boldsymbol{X}_n\right)$ 的子矩阵 $\left(\boldsymbol{X}_1, \boldsymbol{X}_{1+n_1}, \boldsymbol{X}_{1+n_1+n_2}\right)$ 的行向量中出现的次数分别为 b_{i1}、b_{i2}、b_{i3}、b_{i4}、b_{i5}、b_{i6}、b_{i7}、b_{i8}，其中 n_1, n_2 是正整数且 $n_1 + n_2 \leqslant n - 1$，则 $\boldsymbol{O}_n(\boldsymbol{x})$ 的 3-重分布矩阵 $\boldsymbol{B}^3_{\boldsymbol{O}_n(\boldsymbol{x})}$ 可表示为：

$$\boldsymbol{B}^3_{\boldsymbol{O}_n(\boldsymbol{x})} = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} & b_{17} & b_{18} \\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26} & b_{27} & b_{28} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{N1} & b_{N2} & b_{N3} & b_{N4} & b_{N5} & b_{N6} & b_{N7} & b_{N8} \end{pmatrix} = \left(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4, \boldsymbol{b}_5, \boldsymbol{b}_6, \boldsymbol{b}_7, \boldsymbol{b}_8\right) \tag{9}$$

其中，$N = \mathrm{C}_{n-1}^2$。

证明　任取两个正整数 n_1, n_2，满足 $n_1 + n_2 \leqslant n - 1$。选择轨道矩阵 $\boldsymbol{O}_n(\boldsymbol{x})$ 的第 1、$1 + n_1$、$1 + n_1 + n_2$ 列组成子矩阵，若 $\boldsymbol{O}_n(\boldsymbol{x})$ 的任意列数为 3 的子矩阵 $\left(\boldsymbol{X}_i, \boldsymbol{X}_j, \boldsymbol{X}_t\right)$ 满足：

$$\begin{aligned} j - i &\equiv n_1 (\bmod n) \\ t - j &\equiv n_2 (\bmod n) \\ i - t &\equiv n - (n_1 + n_2) (\bmod n) \end{aligned} \tag{10}$$

根据文献[16]，存在一个置换矩阵 $\boldsymbol{P}$，使 $\boldsymbol{X}_i =$

$\boldsymbol{P}^{i-1}\boldsymbol{X}_1$，$\boldsymbol{X}_j=\boldsymbol{P}^{j-n_1-1}\boldsymbol{X}_{1+n_1}=\boldsymbol{P}^{i-1}\boldsymbol{X}_{1+n_1}$，$\boldsymbol{X}_t=\boldsymbol{P}^{t-n_1-n_2-1}\boldsymbol{X}_{1+n_1+n_2}=\boldsymbol{P}^{i-1}\boldsymbol{X}_{1+n_1+n_2}$，即$\left(\boldsymbol{X}_i,\boldsymbol{X}_j,\boldsymbol{X}_t\right)=\boldsymbol{P}^{i-1}\left(\boldsymbol{X}_1,\boldsymbol{X}_{1+n_1},\boldsymbol{X}_{1+n_1+n_2}\right)$。因此，$\left(\boldsymbol{X}_i,\boldsymbol{X}_j,\boldsymbol{X}_t\right)$与$\left(\boldsymbol{X}_1,\boldsymbol{X}_{1+n_1},\boldsymbol{X}_{1+n_1+n_2}\right)$中的每个3-重分布出现的次数相同。将满足式(10)的所有列数为3的子矩阵记作一个集合，其中$\left(\boldsymbol{X}_1,\boldsymbol{X}_{1+n_1},\boldsymbol{X}_{1+n_1+n_2}\right)$为该集合的代表子矩阵。

n_1,n_2的所有取值情况如表1所示。记N为轨道矩阵$\boldsymbol{O}_n(\boldsymbol{x})$中所有列数为3的代表子矩阵的总个数，则有：

$$N=(n-2)+(n-3)+\cdots+1=\frac{(n-1)(n-2)}{2}=\mathrm{C}_{n-1}^2 \tag{11}$$

证毕。

表1 n_1,n_2的所有取值情况

n_1	n_2	代表子矩阵	总数/个
1	1	$(\boldsymbol{X}_1,\boldsymbol{X}_2,\boldsymbol{X}_3)$	
1	2	$(\boldsymbol{X}_1,\boldsymbol{X}_2,\boldsymbol{X}_4)$	
1	3	$(\boldsymbol{X}_1,\boldsymbol{X}_2,\boldsymbol{X}_5)$	$n-2$
⋮	⋮	⋮	
1	$n-2$	$(\boldsymbol{X}_1,\boldsymbol{X}_2,\boldsymbol{X}_n)$	
2	1	$(\boldsymbol{X}_1,\boldsymbol{X}_3,\boldsymbol{X}_4)$	
2	2	$(\boldsymbol{X}_1,\boldsymbol{X}_3,\boldsymbol{X}_5)$	
2	3	$(\boldsymbol{X}_1,\boldsymbol{X}_3,\boldsymbol{X}_6)$	$n-3$
⋮	⋮	⋮	
2	$n-3$	$(\boldsymbol{X}_1,\boldsymbol{X}_3,\boldsymbol{X}_n)$	
		⋮	
$n-2$	1	$(\boldsymbol{X}_1,\boldsymbol{X}_{n-1},\boldsymbol{X}_n)$	1

例1 计算$\boldsymbol{O}_5(\boldsymbol{x})$的3-重分布矩阵，其中$\boldsymbol{x}=(1,0,0,0,0)$。

首先由$\boldsymbol{x}=(1,0,0,0,0)\in\boldsymbol{F}_2^5$，根据轨道矩阵的定义，通过循环左移变换得到轨道矩阵：

$$\boldsymbol{O}_5(\boldsymbol{x})=\begin{pmatrix}1&0&0&0&0\\0&0&0&0&1\\0&0&0&1&0\\0&0&1&0&0\\0&1&0&0&0\end{pmatrix}=(\boldsymbol{X}_1,\boldsymbol{X}_2,\boldsymbol{X}_3,\boldsymbol{X}_4,\boldsymbol{X}_5) \tag{12}$$

根据定理1，写出所有代表子矩阵的3-重分布。以$(\boldsymbol{X}_1,\boldsymbol{X}_2,\boldsymbol{X}_3)$为例，3-重$(0,0,0)$、$(0,0,1)$、$(0,1,0)$、$(0,1,1)$、$(1,0,0)$、$(1,0,1)$、$(1,1,0)$、$(1,1,1)$在子矩阵$(\boldsymbol{X}_1,\boldsymbol{X}_2,\boldsymbol{X}_3)$中出现的次数依次为2、1、1、0、1、0、0、0，则$\boldsymbol{B}_{\boldsymbol{O}_5(\boldsymbol{x})}^3$的第一行为(2, 1, 1, 0, 1, 0, 0, 0)，且代表子矩阵的个数（即3-重分布矩阵的行数）为$\mathrm{C}_4^2=6$，所以$\boldsymbol{O}_5(\boldsymbol{x})$的3-重分布矩阵为：

$$\boldsymbol{B}_{\boldsymbol{O}_5(\boldsymbol{x})}^3=\begin{pmatrix}2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\end{pmatrix} \tag{13}$$

采用类似的方法，可以计算所有的$\boldsymbol{O}_5(\boldsymbol{x})$的3-重分布矩阵，如表2所示。

推论1 任取$\boldsymbol{x}\in\boldsymbol{F}_2^n$，轨道$\boldsymbol{O}_n(\bar{\boldsymbol{x}})$的3-重分布矩阵为：

$$\boldsymbol{B}_{\boldsymbol{O}_n(\bar{\boldsymbol{x}})}^3=(\boldsymbol{b}_8,\boldsymbol{b}_7,\boldsymbol{b}_6,\boldsymbol{b}_5,\boldsymbol{b}_4,\boldsymbol{b}_3,\boldsymbol{b}_2,\boldsymbol{b}_1) \tag{14}$$

证明 对于任意的$\boldsymbol{x}=\left(x_1,x_2,\cdots,x_n\right)\in\boldsymbol{F}_2^n$，$\bar{\boldsymbol{x}}=\left(\boldsymbol{x}_1\oplus1,\boldsymbol{x}_2\oplus1,\cdots,\boldsymbol{x}_n\oplus1\right)$，由$\boldsymbol{O}_n(\boldsymbol{x})=\left(\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_n\right)$，易知$\boldsymbol{O}_n(\bar{\boldsymbol{x}})=\left(\bar{\boldsymbol{X}}_1,\bar{\boldsymbol{X}}_2,\cdots,\bar{\boldsymbol{X}}_n\right)$，设多重集$R$和$N$分别表示$\left(\boldsymbol{X}_1,\boldsymbol{X}_{1+n_1},\boldsymbol{X}_{1+n_1+n_2}\right)$和$\left(\bar{\boldsymbol{X}}_1,\bar{\boldsymbol{X}}_{1+n_1},\bar{\boldsymbol{X}}_{1+n_1+n_2}\right)$中所有的行向量，则多重集$R$和$N$的元素之间存在一一对应关系，即：

$$\begin{gathered}R\leftrightarrow N\\(0,0,0)\leftrightarrow(1,1,1)\\(0,0,1)\leftrightarrow(1,1,0)\\(0,1,0)\leftrightarrow(1,0,1)\\(0,1,1)\leftrightarrow(1,0,0)\\(1,0,0)\leftrightarrow(0,1,1)\\(1,0,1)\leftrightarrow(0,1,0)\\(1,1,0)\leftrightarrow(0,0,1)\\(1,1,1)\leftrightarrow(0,0,0)\end{gathered} \tag{15}$$

根据定理1可知$\boldsymbol{B}_{\boldsymbol{O}_n(\bar{\boldsymbol{x}})}^3=(\boldsymbol{b}_8,\boldsymbol{b}_7,\boldsymbol{b}_6,\boldsymbol{b}_5,\boldsymbol{b}_4,\boldsymbol{b}_3,\boldsymbol{b}_2,\boldsymbol{b}_1)$，证毕。

引理2 设f是n元旋转对称布尔函数，$\mathrm{supp}(f)=(\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_n)$是$f$的支撑矩阵，则$f$是3-CI当且仅当$\left(\boldsymbol{c}_1,\boldsymbol{c}_{1+n_1},\boldsymbol{c}_{1+n_1+n_2}\right)$是一个$\mathbf{OA}\left(|\mathrm{supp}(f)|,3,2,3\right)$，其中$n_1,n_2$是正整数且$n_1+n_2\leqslant n-1$。特别地，当且仅当$|\mathrm{supp}(f)|=2^{n-1}$时$f$是3-弹性函数。

表2　F_2^5上轨道代表元及其3-重分布矩阵

编号	轨道代表元	3-重分布矩阵
(1)	(0,0,0,0,0)	$\begin{pmatrix}1&0&0&0&0&0&0&0\\1&0&0&0&0&0&0&0\\1&0&0&0&0&0&0&0\\1&0&0&0&0&0&0&0\\1&0&0&0&0&0&0&0\\1&0&0&0&0&0&0&0\end{pmatrix}$
(2)	(1,0,0,0,0)	$\begin{pmatrix}2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\\2&1&1&0&1&0&0&0\end{pmatrix}$
(3)	(1,1,0,0,0)	$\begin{pmatrix}1&1&0&1&1&0&1&0\\0&2&1&0&1&0&1&0\\1&1&1&0&0&1&1&0\\0&1&1&1&2&0&0&0\\0&1&2&0&1&1&0&0\\1&0&1&1&1&1&0&0\end{pmatrix}$
(4)	(1,1,1,0,0)	$\begin{pmatrix}0&1&0&1&1&0&1&1\\0&1&0&1&0&1&2&0\\0&1&1&0&0&1&1&1\\0&0&0&2&1&1&1&0\\0&0&1&1&0&2&1&0\\0&0&1&1&1&1&0&1\end{pmatrix}$
(5)	(1,0,1,0,0)	$\begin{pmatrix}0&1&2&0&1&1&0&0\\1&0&1&1&1&1&0&0\\0&1&1&1&2&0&0&0\\1&1&1&0&0&1&1&0\\1&1&0&1&1&0&1&0\\0&2&1&0&1&0&1&0\end{pmatrix}$
(6)	(1,1,0,1,0)	$\begin{pmatrix}0&0&1&1&0&2&1&0\\0&0&1&1&1&1&0&1\\0&0&0&2&1&1&1&0\\0&1&1&0&0&1&1&1\\0&1&0&1&1&0&1&1\\0&1&0&1&0&1&2&0\end{pmatrix}$
(7)	(1,1,1,1,0)	$\begin{pmatrix}0&0&0&1&0&1&1&2\\0&0&0&1&0&1&1&2\\0&0&0&1&0&1&1&2\\0&0&0&1&0&1&1&2\\0&0&0&1&0&1&1&2\\0&0&0&1&0&1&1&2\end{pmatrix}$
(8)	(1,1,1,1,1)	$\begin{pmatrix}0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1\end{pmatrix}$

证明　首先，若f是3-CI的，则$\mathrm{supp}(f)=(\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_n)$构成一个$\mathbf{OA}(|\mathrm{supp}(f)|,n,2,3)$，于是$(\boldsymbol{c}_1,\boldsymbol{c}_{1+n_1},\boldsymbol{c}_{1+n_1+n_2})$是一个$\mathbf{OA}(|\mathrm{supp}(f)|,3,2,3)$。其次，若$(\boldsymbol{c}_1,\boldsymbol{c}_{1+n_1},\boldsymbol{c}_{1+n_1+n_2})$是一个$\mathbf{OA}(|\mathrm{supp}(f)|,3,2,3)$，则由定理1的证明可知，满足式(10)的$(\boldsymbol{c}_i,\boldsymbol{c}_j,\boldsymbol{c}_t)$也是一个$\mathbf{OA}(|\mathrm{supp}(f)|,3,2,3)$，这就蕴含了以$(\boldsymbol{c}_1,\boldsymbol{c}_{1+n_1},\boldsymbol{c}_{1+n_1+n_2})$为代表子矩阵的集合中每个元素都是$\mathbf{OA}(|\mathrm{supp}(f)|,3,2,3)$。当$n_1,n_2$取遍表1的所有情况时，$\mathrm{supp}(f)$的任意列数为3的子矩阵均为$\mathbf{OA}(|\mathrm{supp}(f)|,3,2,3)$，即$\mathrm{supp}(f)$是一个$\mathbf{OA}(|\mathrm{supp}(f)|,n,2,3)$，于是$f$是3-CI的。特别地，当且仅当$|\mathrm{supp}(f)|=2^{n-1}$时$f$是3-弹性函数，证毕。

2.2　利用3-重分布矩阵间接构造

对于任意$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\boldsymbol{F}_2^n$，本节选择如下两个$n$元旋转对称$(n-1)$-弹性函数：

$$f_1(\boldsymbol{x})=x_1\oplus x_2\oplus\cdots\oplus x_n \tag{16}$$

$$f_2(\boldsymbol{x})=f_1(\boldsymbol{x})\oplus 1 \tag{17}$$

f_1和f_2的支撑集分别为$\mathrm{supp}(f_1)=(\boldsymbol{x}\in\boldsymbol{F}_2^n|\mathrm{wt}(\boldsymbol{x})$为奇数)和$\mathrm{supp}(f_2)=(\boldsymbol{x}\in\boldsymbol{F}_2^n|\mathrm{wt}(\boldsymbol{x})$为偶数)，假设存在集合$T$使$T=T_1\cup T_2\subseteq\boldsymbol{F}_2^n$，其中$T_1,T_2$是一些轨道的并集，且$T_1\subseteq\mathrm{supp}(f_1)$，$T_2\subseteq\mathrm{supp}(f_2)$，通过修改$f_1$的支撑集，本文构造一个新函数：

$$f(\boldsymbol{x})=\begin{cases}f_1(\boldsymbol{x})\oplus 1,\boldsymbol{x}\in T\\ f_1(\boldsymbol{x}),\text{其他}\end{cases} \tag{18}$$

定理2　令$n\geqslant 5$是一个正整数，则f是n元旋转对称3-弹性函数当且仅当存在子集合T_1和T_2使它们的3-重分布矩阵满足$\boldsymbol{B}_{T_1}^3=\boldsymbol{B}_{T_2}^3$。

证明　由引理2可知，f是n元旋转对称3-弹性函数当且仅当f的支撑矩阵$\mathrm{supp}(f)$是一个$\mathrm{OA}(2^{n-1},n,2,3)$，即$f$是$n$元旋转对称3-弹性函数当且仅当：

$$\boldsymbol{B}_{\mathrm{supp}(f)}^3=\sum_{\boldsymbol{O}_n(\boldsymbol{x})\subseteq\mathrm{supp}(f)}\boldsymbol{B}_{\boldsymbol{O}_n(\boldsymbol{x})}^3=\begin{pmatrix}2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}\\2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}\\\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}&2^{n-4}\end{pmatrix}_{N\times 8} \tag{19}$$

由于$\mathrm{supp}(f)$和$\mathrm{supp}(f_1)$的3-重分布矩阵分别为 $\boldsymbol{B}^3_{\mathrm{supp}(f)}=\boldsymbol{B}^3_{T_2}+\boldsymbol{B}^3_{\mathrm{supp}(f_1)\setminus T_1}$ 和 $\boldsymbol{B}^3_{\mathrm{supp}(f_1)}=\boldsymbol{B}^3_{T_1}+\boldsymbol{B}^3_{\mathrm{supp}(f_1)\setminus T_1}$，其中$\mathrm{supp}(f)\setminus T_1$表示子集合$T_1$在$\mathrm{supp}(f)$的补集，从而得到$\boldsymbol{B}^3_{\mathrm{supp}(f)}-\boldsymbol{B}^3_{\mathrm{supp}(f_1)}=\boldsymbol{B}^3_{T_2}-\boldsymbol{B}^3_{T_1}$，因此$\boldsymbol{B}^3_{T_1}=\boldsymbol{B}^3_{T_2}$当且仅当$\boldsymbol{B}^3_{\mathrm{supp}(f)}=\boldsymbol{B}^3_{\mathrm{supp}(f_1)}$，从而$f$是$n$元旋转对称3-弹性函数当且仅当存在$T_1$和$T_2$满足$\boldsymbol{B}^3_{T_1}=\boldsymbol{B}^3_{T_2}$，证毕。

例2 已知$f_1(\boldsymbol{x})=\oplus_{i=1}^{5}x_i$是旋转对称4-弹性函数，现利用3-重分布矩阵对该函数进行二次构造，具体步骤如下。

首先，表2中列出了所有5元向量的3-重分布矩阵。

其次，根据定理2，任取集合T_1中的两个轨道，代表元为(1,0,0,0,0)和(1,1,1,0,0)，考虑它们的3-重分布矩阵之和为：

$$\boldsymbol{B}=\begin{pmatrix}2&2&1&1&2&0&1&1\\2&2&1&1&1&1&2&0\\2&2&2&0&1&1&1&1\\2&1&1&2&2&1&1&0\\2&1&2&1&1&2&1&0\\2&1&2&1&2&1&0&1\end{pmatrix} \tag{20}$$

经搜索计算可知，集合T_2中不存在任何两个轨道的3-重分布矩阵之和等于$\boldsymbol{B}$。更一般地，对于满足条件$|T_1|=|T_2|$的任意集合T_1,T_2，通过计算可验证等式$\boldsymbol{B}^3_{T_1}=\boldsymbol{B}^3_{T_2}$均不成立。这表明不存在新的旋转对称3-弹性函数。

2.3 利用正交表直接构造

将矩阵$\boldsymbol{A}=(a_{ij})_{n\times m}$和$\boldsymbol{B}=(b_{ij})_{n\times m}$的Schur积记作$\boldsymbol{A}\circ\boldsymbol{B}=(a_{ij}b_{ij})_{n\times m}$，则有：

$$\boldsymbol{U}=\begin{pmatrix}\boldsymbol{u}_0\\\boldsymbol{u}_1\\\vdots\\\boldsymbol{u}_{2^n-1}\end{pmatrix}_{2^n\times n}=\begin{pmatrix}0&0&\cdots&0\\0&0&\cdots&1\\\vdots&\vdots&&\vdots\\1&1&\cdots&1\end{pmatrix}_{2^n\times n}=(u_{ij})_{2^n\times n} \tag{21}$$

其中，$1\leqslant i\leqslant 2^n$，$1\leqslant j\leqslant n$。定义[16]：

$$\boldsymbol{V}=(v_{ij})_{2^n\times n}=((-1)^{u_{ij}})_{2^n\times n}=\begin{pmatrix}1&1&\cdots&1\\1&1&\cdots&-1\\\vdots&\vdots&&\vdots\\-1&-1&\cdots&-1\end{pmatrix}_{2^n\times n}=(\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n) \tag{22}$$

$$\boldsymbol{V}_2=\left(\boldsymbol{v}_1\circ\boldsymbol{v}_2,\boldsymbol{v}_1\circ\boldsymbol{v}_3,\cdots,\boldsymbol{v}_1\circ\boldsymbol{v}_{\left\lceil\frac{(n+1)}{2}\right\rceil}\right) \tag{23}$$

$$\boldsymbol{V}_3=(\boldsymbol{v}_1\circ\boldsymbol{v}_2\circ\boldsymbol{v}_3,\boldsymbol{v}_1\circ\boldsymbol{v}_2\circ\boldsymbol{v}_4,\cdots,\boldsymbol{v}_1\circ\boldsymbol{v}_{n-1}\circ\boldsymbol{v}_n) \tag{24}$$

定理3 设$C_{2^n-1}=\{2^n-1\}$为一个特殊的分圆陪集，令$\Gamma_2^+(n)=\{$所有Z_{2^n-1}中的陪集首$\}\cup C_{2^n-1}$，则n元布尔函数f是旋转对称3-弹性函数当且仅当方程组：

$$\begin{cases}\sum\limits_{s\in\Gamma_2^+(n)}n_s\cdot y_s=2^{n-1}\\\sum\limits_{s\in\Gamma_2^+(n)}n_s\cdot\dfrac{\mathrm{wt}(\boldsymbol{v}_s)}{n}\cdot y_s=2^{n-2}\\(y_0,y_1,\cdots,y_{2^n-1})\boldsymbol{V}_2=\boldsymbol{0}_{\left\lceil\frac{(n-1)}{2}\right\rceil}\\(y_0,y_1,\cdots,y_{2^n-1})\boldsymbol{V}_3=\boldsymbol{0}_N\end{cases} \tag{25}$$

至少有一个解。

证明 由文献[16]可知，f是旋转对称2-弹性函数当且仅当方程组的前3个等式至少有一个解，因此，证明定理3等价于已知f是n元旋转对称2-弹性布尔函数，证明f是旋转对称3-弹性函数当且仅当$(y_0,y_1,\cdots,y_{2^n-1})\boldsymbol{V}_3=\boldsymbol{0}_N$有解。

若$(y_0,y_1,\cdots,y_{2^n-1})\boldsymbol{V}_3=\boldsymbol{0}_N$有解，由引理2，仅需证明$\left(\boldsymbol{c}_1,\boldsymbol{c}_{1+n_1},\boldsymbol{c}_{1+n_1+n_2}\right)$是一个$\mathbf{OA}(2^{n-1},3,2,3)$。已知$f$是旋转对称2-弹性函数，则$\left(\boldsymbol{c}_1,\boldsymbol{c}_{1+n_1},\boldsymbol{c}_{1+n_1+n_2}\right)$是一个$\mathbf{OA}(2^{n-1},3,2,2)$，即：

$$\begin{cases}N_0+N_1=N_2+N_3=N_4+N_5=N_6+N_7=2^{n-3}\\N_0+N_2=N_1+N_3=N_4+N_6=N_5+N_7=2^{n-3}\\N_0+N_4=N_1+N_5=N_2+N_6=N_3+N_7=2^{n-3}\end{cases} \tag{26}$$

根据$(y_0,y_1,\cdots,y_{2^n-1})\boldsymbol{V}_3=\boldsymbol{0}_N$可知：

$$N_0+N_3+N_5+N_6=N_1+N_2+N_4+N_7=2^{n-2} \tag{27}$$

经计算可得：

$$N_0=N_1=N_2=N_3=N_4=N_5=N_6=N_7=2^{n-4} \tag{28}$$

故$\left(\boldsymbol{c}_1,\boldsymbol{c}_{1+n_1},\boldsymbol{c}_{1+n_1+n_2}\right)$是一个$\mathbf{OA}(2^{n-1},3,2,3)$。

若f是旋转对称3-弹性函数，则对任意的$\boldsymbol{\alpha}\in F_2^n$满足$\mathrm{supp}(\boldsymbol{\alpha})=\{1,1+n_1,1+n_1+n_2\}$，有$W_f(\boldsymbol{\alpha})=0$。由式(4)可得$S_f(\boldsymbol{\alpha})=0$，即$(y_0,y_1,\cdots,y_{2^n-1})(\boldsymbol{u}_1\circ\boldsymbol{u}_{1+n_1}\circ\boldsymbol{u}_{1+n_1+n_2})=0$。当$n_1,n_2$取遍表1中各种可能的取值时，等式$(y_0,y_1,\cdots,y_{2^n-1})\boldsymbol{V}_3=\boldsymbol{0}_N$成立，证毕。

3　结束语

本文围绕旋转对称3-弹性函数的构造与刻画问题展开研究。通过引入旋转对称轨道的3-重分布矩阵，提出了一种间接构造旋转对称3-弹性函数的方法，并证明了其可行性。同时，基于弹性函数与正交表之间的关系，将旋转对称3-弹性函数的构造问题转化为特定代数方程组的求解问题，为此类函数的系统性构造提供了另一条理论路径。

参考文献：

[1] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[2] Ding C S, Xiao G Z, Shan W J. The stability theory of stream ciphers[M]. Berlin: Springer, 1991.

[3] Matsui M. Linear cryptanalysis method for DES cipher[C]//Advances in Cryptology-EUROCRYPT'93. Berlin: Springer, 1994: 386-397.

[4] Siegenthaler T. Decrypting a class of stream ciphers using ciphertext only[J]. IEEE Transactions on Computers, 1985, 34(1): 81-85.

[5] Lai X J. Higher order derivatives and differential cryptanalysis[M]//Blahut R E, Costello D J, Maurer U, et al. Communications and cryptography: two sides of one tapestry. Boston: Springer US, 1994: 227-233.

[6] Filiol E, Fontaine C. Highly nonlinear balanced Boolean functions with a good correlation-immunity[C]//Advances in Cryptology-EUROCRYPT'98. Berlin: Springer, 1998: 475-488.

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

[8] Cusick T W, Stanica P. Cryptographic Boolean functions and applications[M]. San Diego: Academic Press, 2017.

[9] Fontaine C. On some cosets of the first-order Reed-Muller code with high minimum weight[J]. IEEE Transactions on Information Theory, 1999, 45(4): 1237-1243.

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

[11] 李泉, 高光普, 刘文芬. k-阶旋转对称函数性质分析与轨道计数[J]. 通信学报, 2012, 33(1): 114-119.
Li Q, Gao G P, Liu W F. Analysis of properties and counting of orbits for k-rotation symmetric Boolean functions[J]. Journal on Communications, 2012, 33(1): 114-119.

[12] Fu S J, Li C, Matsuura K, et al. Construction of even-variable rotation symmetric Boolean functions with maximum algebraic immunity[J]. Science China Information Sciences, 2013, 56(3): 4350.

[13] Chen Y D, Lin L M, Liao L M, et al. Constructing higher nonlinear odd-variable RSBFs with optimal AI and almost optimal FAI[J]. IEEE Access, 2019, 7: 133335-133341.

[14] Stănică P, Maitra S, Clark J A. Results on rotation symmetric bent and correlation immune Boolean functions[C]//Proceedings of the International Workshop on Fast Software Encryption. Berlin: Springer, 2004: 161-177.

[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] 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.

[17] 杜蛟, 李琳, 赵紫薇, 等. 7元旋转对称2-弹性函数的构造[J]. 通信学报, 2024, 45(1): 194-200.
Du J, Li L, Zhao Z W, et al. Concrete constructions of 2-resilient rotation symmetric Boolean functions with 7 variables[J]. Journal on Communications, 2024, 45(1): 194-200.

[18] 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.

[19] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications[J]. IEEE Transactions on Information Theory, 1984, 30(5): 776-780.

[20] Chor B, Goldreich O, Hasted J, et al. The bit extraction problem or t-resilient functions[C]//Proceedings of the 26th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1985: 396-407.

[21] Stinson D R. Resilient functions and large sets of orthogonal arrays[J]. Congressus Numerantium, 1993, 92: 105-110.

[22] Sun L, Liu J, Fu F W. Secondary constructions of RSBFs with good cryptographic properties[J]. Information Processing Letters, 2019, 147: 44-48.

[23] Du J, Fu S J, Qu L J, et al. A novel construction of 2-resilient rotation symmetric Boolean functions[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2022, 105 (2): 93-99.

[24] Du J, Li L, Fu S J, et al. Constructions of 2-resilient rotation symmetric Boolean functions with odd number of variables[J]. Theoretical Computer Science, 2024, 991: 114429.

[25] Camion P, Carlet C, Charpin P, et al. On correlation-immune functions [C]//Advances in Cryptology-CRYPTO'91. Berlin: Springer, 2007: 86-100.

[26] 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. Analysis of security index of cryptographic function[M]. Beijing: Science Press, 2011.

[作者简介]

张慧（1994– ），女，博士，河南师范大学讲师，主要研究方向为编码密码的数学理论。

杜蛟（1978– ），男，博士，河南师范大学副教授、博士生导师，主要研究方向为编码密码的数学理论。

陈晓婷（2001– ），女，河南师范大学硕士生，主要研究方向为密码函数的设计与安全性分析。

李功丽（1981– ），女，博士，河南师范大学副教授，主要研究方向为分组密码、隐私计算和联邦学习。

王宏盼（2003– ），男，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。

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