具有最优代数免疫度和高非线性度的奇变元 RSBFs 搜索

王 勇[1] 周 丹[1] 何常乐[1] 邵 峥[1] 李金鹏[1]
WANG Yong ZHOU Dan HE Changle SHAO Zheng LI Jinpeng

摘 要 基于旋转对称布尔函数（RSBFs）优良的结构和高效的硬件实现特性，寻找具有多种优良密码学性质的该类布尔函数一直是密码学和信息安全领域的重要课题。代数免疫度和非线性度是衡量布尔函数安全性的关键指标，但已有成果中两者难以同时兼具。基于此，文章提出两阶段轨道遗传算法（TOGA），设计了基于循环轨道的结构化编码、约束保持的遗传算子、两阶段筛选机制等创新策略，有效解决了大规模空间中多目标优化问题。实验结果表明，对于 n=5, 7, 9, 11, 13, 15 的奇变元，所提算法搜索到的 RSBFs 具有最优代数免疫度，非线性度优于现有同类函数，代数次数达到了 n−2。该研究为密码系统中布尔函数的设计提供了新思路。

关键词 旋转对称布尔函数；代数免疫度；非线性度；遗传算法；密码学

doi：10.3969/j.issn.1672-9528.2026.08.008

0 引言

密码学在网络信息安全领域扮演着关键角色，布尔函数是流密码和分组密码的核心组件，其密码学性质的好坏直接影响密码系统的安全性 [1]。为抵抗各种攻击，用于密码系统的布尔函数通常需要具有平衡性、高非线性度、高代数次数等密码学特性。Courtois 等 [2] 提出代数攻击之后，代数免疫度（algebraic immunity, AI）成为评判布尔函数抵抗代数攻击能力的指标。

旋转对称布尔函数（rotation symmetric boolean functions, RSBFs）是一类函数值在输入循环移位下保持不变的布尔函数，因其硬件实现上的高效性而受到广泛关注 [3-4]。该类函数在一定条件下可以具有优良密码学性质，比如已知 1 阶弹性函数 [5]，以及作为 SHA-3 标准 Keccak 中唯一的非线性部件的布尔函数 [6] 都是 RSBFs。代数免疫度最优的奇变元布尔函数是布尔函数方向的研究热点，涌现了很多成果 [7-11]。然而，已有成果的非线性度仍有提升空间。因此，研究具有最优代数免疫度同时具有高非线性度的 RSBFs 仍有重要的理论和现实意义。

针对上述问题，本文在遗传算法 [12-13] 的基础上，提出两阶段轨道遗传算法（two-stage orbit-based genetic algorithm, TOGA）。该算法针对 RSBFs 的循环轨道结构，设计了基于轨道子集的结构化编码方式，将搜索空间从2^{2^n}降低到2^{g_n}（g_n 为轨道数）；同时设计了约束保持的遗传算子，确保进化过程中所有个体均满足平衡性约束；并通过两阶段筛选机制——第一阶段快速筛选满足 AI 必要条件的候选；第二阶段精确验证 AI——实现代数免疫度和非线性度的联合优化。并对 n=5, 7, 9, 11, 13, 15 变元的奇变元函数进行搜索，搜索到具有多种优良密码学性质的 RSBFs。

1 预备知识

1.1 布尔函数基础

首先给出布尔函数的定义，设 n 表示正整数，F_2^n 表示 n 维二元向量空间。n 元布尔函数 f：$F_2^n \to F_2$ 可以用真值表 $f=(f(0,0,\cdots,0), f(0,0,\cdots,1), \cdots, f(1,1,\cdots,1))$ 来表示。布尔函数 f 的汉明重量定义为 $\mathrm{wt}(f)=|\{\boldsymbol{x}\in F_2^n \mid f(\boldsymbol{x})=1\}|$。对任意布尔函数 f，除真值表之外，还可以用代数正规型唯一表示，即：

$$f(\boldsymbol{x})=\bigoplus_{\boldsymbol{u}\in F_2^n} a_{\boldsymbol{u}}\left(\prod_{i=1}^{n} x_i^{u_i}\right) \tag{1}$$

式中：$a_{\boldsymbol{u}}\in F_2$，$\oplus$ 表示 F_2 上的加法。

对于 $\boldsymbol{x}=(x_1, x_2,\cdots, x_{n-1})\in F_2^n$，定义循环移位操作 $\rho(\boldsymbol{x})=(x_1, x_2,\cdots, x_{n-1}, x_0)$。若对任意 $\boldsymbol{x}\in F_2^n$ 和任意正整数 k，有 $f(\rho^k(\boldsymbol{x}))=f(\boldsymbol{x})$，则称布尔函数 f 为旋转对称布尔函数。对于 $\boldsymbol{x}\in F_2^n$，$\boldsymbol{x}$ 的循环轨道定义为：$O(\boldsymbol{x})=\{\boldsymbol{x}, \rho(\boldsymbol{x}), \rho^2(\boldsymbol{x}),\cdots, \rho^{n-1}(\boldsymbol{x})\}$，则不难发现 RSBFs 的真值表由循环轨道决定，选择若干轨道的并集作为函数的支撑集，即可构造得到 RSBFs。

1. 信阳学院计算机与人工智能学院 河南信阳 464000
[基金项目] 信阳学院 2025 年校级科研项目“旋转对称密码函数的构造与分析研究”（2025-XJLYB-005）

1.2 密码学指标

定义 1（非线性度）：布尔函数 f 的非线性度定义为：

$$\mathrm{nl}(f)=2^{n-1}-\frac{1}{2}\max_{\omega\in F_2^n}|\hat{f}(\omega)| \tag{2}$$

式中：$\hat{f}(\omega)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus\omega\cdot x}$ 是 Walsh 变换。且已知对任意奇变元函数 f，有 $\mathrm{nl}(f)\le 2^{n-1}-2^{(n-1)/2}$。

定义 2（代数免疫度）[4]：布尔函数 f 的代数免疫度 AI(f) 定义为 f 或 $f\oplus 1$ 的零化子的最低次数，即：

$$\mathrm{AI}(f)=\min_{g\neq 0}\{\deg(g)|\ fg=0 \text{ 或 } (f\oplus 1)g=0\} \tag{3}$$

且对任意 n 元布尔函数，有 $\mathrm{AI}(f)\le\lceil n/2\rceil$。若满足 $\mathrm{AI}(f)=\lceil n/2\rceil$，则称 f 具有最优代数免疫度。

定理 1（最优 AI 的必要条件）：设 n 为奇数，$g\in B_n$。若满足 $\mathrm{AI}(g)=\lceil n/2\rceil$，则对于所有 $2\le i\le n-1$，有 $\mathrm{wt}(g|_{V_{n,i}})\neq 0$ 且 $\mathrm{wt}(g|_{V_{n,i}})\neq|V_{n,i}|$，其中 $V_{n,i}$ 是 F_2^n 中汉明重量为 i 的所有向量构成的集合。

2 两阶段轨道遗传算法

在 RSBFs 领域，面临搜索空间随变元数超指数增长、代数免疫度与非线性度的联合优化、平衡性约束的满足等多重困难。针对这些问题，本节给出针对性的编码方案、遗传算子和筛选机制。

2.1 基于循环轨道的编码

n 元布尔函数的真值表长度为 2^n，若直接用二进制串编码，搜索空间达 2^{2^n}。RSBFs 的循环对称性意味着同一轨道内的向量取值相同，因此可用轨道子集代替完整真值表。

设 F_2^n 的全部循环轨道为 $\{O_1,O_2,\ldots,O_{g_n}\}$，$g_n$ 为轨道数。旋转对称布尔函数 f 由轨道选择子集 $S\subseteq\{1,2,\ldots,g_n\}$ 唯一确定。

$$f_S(\boldsymbol{x})=\begin{cases}1, & \boldsymbol{x}\in\bigcup_{i\in S}O_i\\ 0, & \text{其他}\end{cases} \tag{4}$$

搜索空间压缩为 2^{g_n}。以 n=13 为例，g_{13}=632，搜索空间从 2^{8192} 降至 2^{632}。

2.2 遗传算子设计

平衡性要求 $\mathrm{wt}(f)=2^{n-1}$，即选中轨道的元素总数恰好为 2^{n-1}，为此本文设计了以下约束保持算子。

（1）种群初始化：对轨道索引作随机排列，按序逐个加入并累加轨道大小，当累加值恰好等于 2^{n-1} 时停止。该过程重复 P 次生成初始种群，每个个体均满足平衡性。

（2）交叉操作：设父代为 S_1、S_2，子代的构造分三步：取公共轨道 $S_\cap=S_1\cap S_2$；将差异轨道 $\Delta=(S_1\setminus S_2)\cup(S_2\setminus S_1)$ 随机打乱；依次将 Δ 中的轨道加入子代，直到总重量达到 2^{n-1}。公共轨道的保留使子代继承父代的共同特征，随机填充则引入多样性。

（3）变异操作：对个体 S，随机选取 $i\in S$ 和 $j\notin S$，满足 $|O_i|=|O_j|$，执行替换 $S'=(S\setminus\{i\})\cup\{j\}$。等重量替换保证变异前后总重量不变，若不存在满足条件的 j，则跳过变异。

（4）适应度函数：适应度函数对个体做分层筛选，首先检查平衡性，再检查 AI 必要条件，两项均通过后计算非线性度：

$$\mathrm{fitness}(S)=\begin{cases}\mathrm{nl}(f_s), & \mathrm{wt}(f_s)=2^{n-1}\ \text{且}\ f_s\text{满足定理1}\\ -1, & \text{其他}\end{cases} \tag{5}$$

2.3 两阶段筛选策略

AI 的精确计算需构造评估矩阵并求秩，复杂度远高于非线性度计算。为兼顾效率与精度，将筛选分为两个阶段。

（1）第一阶段：AI 必要条件快速筛选。在每一代的适应度评估中，利用定理 1 的必要条件进行快速过滤。对每个重量层 $i\in[2,n-1]$，检查 $W_i(f)=\sum_{x\in V_{n,i}}f(\boldsymbol{x})$ 是否满足 $0<W_i(f)<|V_{n,i}|$。该检查仅需遍历真值表，复杂度 $O(2^n)$。

（2）第二阶段：精确 AI 验证。遗传进化收敛后，取非线性度最高的 K 个候选进行精确验证。对候选次数 $d=1,2,\ldots,\lceil n/2\rceil$，构造评估矩阵：

$$\boldsymbol{A}_d=\left(m_j(z_i)\right)_{|Z_f|\times s} \tag{6}$$

式中：$\{m_j\}$ 为次数不超过 d 的单项式集合，$Z_f=\{\boldsymbol{x}\,|\,f(\boldsymbol{x})=1\}$ 为支撑集。在 F_2 上对 $\boldsymbol{A}_d$ 作高斯消元求秩，若 $\mathrm{rank}(\boldsymbol{A}_d)<s$，则 f 存在次数不超过 d 的零化子。对 f 和 $f\oplus 1$ 分别验证，若均不存在次数小于 $\lceil n/2\rceil$ 的零化子，则 $\mathrm{AI}(f)=\lceil n/2\rceil$。

2.4 算法描述

算法 1 为 TOGA 的完整流程。第一阶段通过遗传进化搜索高非线性度候选，第二阶段对候选作精确 AI 验证。

两阶段筛选策略的核心优势在于，第一阶段的必要条件检查开销极低，可在遗传进化的每一代中使用；第二阶段的精确验证仅对少量高非线性度候选执行。实验表明，两阶段策略有效降低了总计算时间。

3 实验

为验证本文 TOGA 的有效性，针对不同规模的搜索问题采用不同的策略。对于 n=5, 7（搜索空间 2^{g_n} 不超过 2^{20}）上运行 TOGA，并与穷举搜索结果对比，验证算法的正确性；

然后在 n=9, 11, 13, 15（搜索空间超过 2^{60}，穷举不可行）上运行 TOGA，验证算法在大规模问题上的有效性。实验在 Intel Core i7 处理器、32 GB 内存环境下运行，采用 Python 3.10 和 NumPy 2.2 实现。TOGA 核心参数设置为：种群规模 $P=200$，最大迭代 $G=1\,000$，变异率 $p_m=0.15$，第二阶段验证候选数 $K=50$。

算法 1 TOGA：两阶段轨道遗传算法

输入：变元数 n，种群大小 P，最大迭代代数 G，变异率 p_m

输出：满足最优 AI 且非线性度高的 RSBFs 集合 R

1. 计算轨道 $\{O_1, O_2, \cdots, O_m\}$，目标重量 $W=2^{n-1}$

2. 生成初始种群$\mathcal{P}$：随机选择轨道使累积重量 $=W$（共 P 个个体）

3. $R\leftarrow\varnothing$，$\mathrm{nl}^*\leftarrow 0$（当前最优非线性度），$t_0\leftarrow 0$（上次改进代数）

4. for $t=1$ to G do

5. for $S\in P$ do

6. if $\mathrm{wt}(f_s)=W$ 且满足 AI 必要条件 then

7. $\mathrm{nl}\leftarrow\mathrm{nl}(f_s)$

8. if $\mathrm{nl}>\mathrm{nl}^*$ then

9. $\mathrm{nl}^*\leftarrow\mathrm{nl}$，$t_0\leftarrow t$，$R\leftarrow R\cup\{S\}$

10. end if

11. end if

12. end for

13. if $t-t_0>50$ then break

14. end if

15. 保留 $P/2$ 个精英个体

16. 通过交叉（公共轨道 + 差异部分填充）和变异（等重量轨道替换）产生 $P/2$ 个子代

17. end for

18. for $S\in R$（按 nl 降序取前 K 个）do

19. if $\mathrm{AI}(f_S)=\lceil n/2\rceil$ then return S

20. end if

21.end for return $\varnothing$

3.1 搜索结果

表 1 将本文 TOGA 搜索得到的代数免疫度最优 RSBFs 的非线性度与同类研究成果进行了对比。其中 nl(f) 为本文搜索到的函数的非线性度，$\mathrm{nl}_{\max}=2^{n-1}-2^{(n-1)/2}$为非线性度理论上界，比率为$\mathrm{nl}(f)/\mathrm{nl}_{\max}$。本文所有函数结果均已通过精确 AI 验证，确认$\mathrm{AI}(f)=\lceil n/2\rceil$。

由表 1 可知，n=5, 7 的 TOGA 搜索结果与穷举搜索一致，非线性度均达到理论上界，验证了 TOGA 算法的正确性；n = 9, 11, 13, 15 的非线性度趋近理论上界，比率在 97% 以上，与择多函数和近年同类最优 AI 研究成果相比效果提升明显。

表 1 代数免疫度最优 RSBFs 非线性度对比

n	择多函数	文献 [7]	文献 [8]	本文 nl(f)	$\mathrm{nl}_{\max}$	比率 /%
5	10	—	—	**12**	12	1.00
7	44	—	—	**56**	56	1.00
9	186	188	—	**236**	240	0.983 3
11	772	782	816	**972**	992	0.979 8
13	3 172	3 208	3 288	**3 992**	4 032	0.990 1
15	12 952	13 064	13 274	**16 024**	16 256	0.985 7

本文搜索得到的 RSBFs 除了具有平衡性、最优代数免疫度、高非线性度之外，同时具有较高的代数次数。表 2 给出了搜索 n=5, 7, 9, 11, 13, 15 变元 RSBFs 的代数次数，其中 deg(f) 表示代数次数，$\deg_{\max}=n-1$ 为平衡函数代数次数理论上界。

从表 2 可以看出，本文搜索得到的 n=5 至 n=15 的奇变元函数，代数次数达到了几乎最优 $n-2$，接近理论上界。

表 2 各变元的代数次数

n	deg(f)	$\deg_{\max}$
5	3	4
7	5	6
9	7	8
11	9	10
13	11	12
15	13	14

为便于验证和复现，n=9 和 n=11 的本文最优函数真值表置于附录。

3.2 算法效率

本文 TOGA 的计算时间主要由两部分组成：第一阶段遗传进化的开销主要由快速 Walsh-Hadamard 变换（FWHT）主导，复杂度为$O(G\cdot P\cdot n\cdot 2^n)$；第二阶段 AI 验证需对每个候选构造多个评估矩阵（对应$d=1,2,\ldots,\lceil n/2\rceil-1$），总开销为$O(K\cdot c(n)\cdot 2^{3n})$。由于第一阶段仅执行必要条件检查而跳过精确 AI 计算，两阶段策略有效降低了总计算时间。对于 n=5, 7，搜索空间较小，时间在秒级；对于 n=9, 11, 13，时间在分钟级；对于 n=15，时间在小时级。总体而言，本文算法运行效率在可接受范围。

4 结语

本文提出了两阶段轨道遗传算法 TOGA，用于搜索同时具有最优代数免疫度和高非线性度的奇变元 RSBFs。算法基于循环轨道编码将搜索空间压缩至2^{g_n}，设计了约束保持的遗传算子和两阶段筛选机制，兼顾搜索效率与验证精度。实验结果表明，本文算法在 n=5, 7, 9, 11, 13, 15 上搜索得到具有最优代数免疫度的 RSBFs，非线性度达到理论上界的 97% 以上，优于现有同类函数。此外，经验证搜索得到的函数代数次数为 $n-2$，达到了几乎最优。本文搜索得到的具有多种优良密码学性质的 RSBFs 可以为轻量级密码算法的设计提供更多可选择的布尔函数。

附录：

9 元真值表：

FFABC89EF0C0C7ADAE51A155A13B99E7C9AD630398
16366298560ECA97C3B96AF186C8B32D1F155B939146684E
287958D285377D55A8A0DCC37FF00E9FC278C8

11 元真值表：

921D57A2733ADD087B1E5BCDE2A314D47E8A06BD32
DBA5F6EC0D980A4720A6752AB98589012C9BE20B1CE78B
CD73BE3CFDA411E3D69041D8617B4D0499297A231C8C9B
87C527D0C704121CE5D2CAAD0851DB47A4AD7ED5CBE4B
62F0FCFB84AF4EEE39D214247AD4AA268C6452003F7D57C
127EDE61F65131969348D36EDD0D1B47F0D4F0D6DB816EE
0274D3EA340B02F0531125816B1BD66F259E49C9DB251C16
253B3CB246BC830DDB23EF9A633B48EA9718B3808AB01F
FE4EE9ED5658DAF35BCECED1A83B61843354C657ACDA6
74D98D592984F46D25621D14011FAA6FB3376AB416497AB
CB2ED3D12EB3876170B578669C64B7494E71F29A9E6B711
A753DE

参考文献：

[1] 郑东，赵庆兰，张应辉 . 密码学综述 [J]. 西安邮电大学学报，2013, 18(6):1-10.

[2]Courtois N T, Meier W. Algebraic attacks on stream ciphers with linear feedback[C]//Advances in Cryptology-EUROCRYPT 2003.Berlin:Springer,2003: 345–359.

[3] 高光普 . 旋转对称布尔函数研究综述 [J]. 密码学报，2017, 4(3): 273-290.

[4] 沈黎鹏，陈克非 . 一类代数免疫度最优的奇数变元旋转对称布尔函数的构造 [J]. 密码学报 ,2019,6(4):526-540.

[5]Pang Shanqi, Xu Wenju, Du Jiao, et al. Construction and count of 1-Resilient rotation symmetric boolean functions on 4p variables[J]. Chinese Journal of Electronics, 2017, 26(6): 1276-1283.

[6]Gao Guangpu, Dongdai, Liu Wenfen .A note on rotation symmetric s-boxes[J]. Journal of Systems Science & Complexity, 2019, 32(5): 1460-1472.

[7] 王丙心 . 两类旋转对称布尔函数的构造 [D]. 开封 : 河南大学 , 2021.

[8] 王勇，郑东，赵庆兰，等 . 一类新的代数免疫度最优的奇变元旋转对称布尔函数的构造 [J]. 密码学报 ,2022,9(4):644-662.

[9] 许豪杰 . 密码学性质优良的布尔函数的启发式算法研究 [D]. 西安 : 长安大学 ,2023.

[10]Su Sihong, Li Jingjing, Wang Bingxin.A new construction of odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and higher nonlinearity[J]. Theoretical Computer Science, 2021,887:152-163.

[11]Guo Fei ,Wang Zilong.Balanced odd-variable rotation symmetric boolean functions with optimal algebraic immunity and higher nonlinearity[J]. Discrete Applied Mathematics,2023,324:18-28.

[12] 张思瑶 . 基于改进模拟退火的布尔函数生成算法 [J]. 网络安全技术与应用 ,2021(7):47-49.

[13] 赵海霞，刘德雄 . 基于 Walsh 谱与真值表关联矩阵 nA 和 nB 的 RSBF 的多指标搜索方法 [J]. 信息网络安全，2025,25(7):1126-1137.

【作者简介】

王勇（1997—），男，河南信阳人，硕士，专任教师、助教，研究方向：密码学、网络信息安全。

（收稿日期：2026-07-07　修回日期：2026-08-07）