# SPS 结构大规模 S 盒设计与分析

张岚[1]，何良生[1,2]，郁滨[1]

（1. 信息工程大学密码工程学院，河南 郑州 450001；2. 国家密码管理局，北京 100036）

**摘 要：**基于循环移位与异或运算构造了有限域$(F_2^m)^4$上的一类最优线性变换 $P$，借鉴线性变换输入输出关系反证法的思想，提出将最优线性变换目标问题转化为若干个递进关系定理的证明方法，不仅解决了该类最优线性变换的证明，而且适用于任意线性变换的证明。通过小规模 S 盒与最优循环移位–异或型线性变换 $P$，建立了 2 轮 SPS 结构的大规模 S 盒模型，设计了一系列密码学性质优良的轻量级大规模 S 盒，仅使用查表、循环移位、异或三类基本运算，提高了大规模 S 盒的线性度和差分均匀度。理论证明和实例分析表明，与已有大规模 S 盒构造方法相比，所提大规模 S 盒设计方案运算代价更加低廉，其差分、线性等密码学性质更加优良，适宜用于轻量级密码算法非线性置换设计。

**关键词：**SPS 结构；大规模 S 盒；循环移位–异或型线性变换

**中图分类号：**TN918.1

**文献标志码：**A

**DOI:** 10.11959/j.issn.1000–436x.2023033

# Large-scale S-box design and analysis of SPS structure

ZHANG Lan[1], HE Liangsheng[1,2], YU Bin[1]

1. Department of Cryptogram Engineering, Information Engineering University, Zhengzhou 450001, China

2. State Cryptography Administration, Beijing 100036, China

**Abstract:** A class of optimal linear transformation $P$ over a finite field $(F_2^m)^4$ was constructed based on cyclic shift and XOR operation. Using the idea of inverse proof of input-output relation of linear transformation for reference, a proof method was put forward that transformed the objective problem of optimal linear transformation into several theorems of progressive relation, which not only solved the proof of that kind of optimal linear transformation, but also was suitable for the proof of any linear transformation. By means of small-scale S-box and optimal cyclic shift-XOR linear transformation $P$, a large-scale S-box model with 2-round SPS structure was established, and a series of lightweight large-scale S-boxes with good cryptographic properties were designed. Only three kind of basic operations such as look-up table, cyclic shift and XOR were used in the proposed design scheme, which improved the linearity and difference uniformity of large-scale S-boxes. Theoretical proof and case analysis show that, compared with the existing large-scale S-box construction methods, the proposed large-scale S-box design scheme has lower computational cost and better cryptographic properties such as difference and linearity, which is suitable for the design of nonlinear permutation coding of lightweight cryptographic algorithms.

**Keywords:** SPS structure, large-scale S-box, cyclic shift-XOR linear transformation

## 0 引言

非线性编码是分组密码算法的主要模块，混淆性能较好的非线性编码设计是分组密码算法研究的重要内容。目前，常用的非线性编码为 S 盒，它是分组密码算法的关键部件，主要提供算法所必需的混淆作用，其密码强度直接影响整个密码算法的安全强度。尤其是大规模 S 盒，其极大地提高了非线性编码的线性度和差分均匀度，可以在较少的轮数内使分组密码达到抵抗差分分析和线性分析的安全界。

大规模 S 盒一般是由小规模 S 盒通过某种结合规则满足一定的约束条件构造的，可分为以下 4 种

**收稿日期：**2022–08–30；**修回日期：**2022–11–18

情形。第一种情形是利用密码学结构如 MISTY、Feistel 或直接由小规模 S 盒并置构造大规模 S 盒，基于 3 轮平衡 Feistel 结构[1-2]、3 轮 Lai-Massey 结构[3]及 3 轮 MISTY 结构[4]构造大规模 S 盒，可使 S 盒密码性质适中并减少硬件资源占用。其中，MISTY[5]使用 2 个 9 bit 置换与一个 7 bit 置换，使用 3 轮 MISTY 结构构造 16 bit 大规模 S 盒，再使用 3 轮 MISTY 结构构造 32 bit 非线性置换，这种嵌套结构可提高整个非线性环节的密码学性质，但需合理选择内嵌的非线性函数。文献[6]提出一种新的 8 bit 轻量化 S 盒设计方法，其单轮逻辑运算仅涉及 4 个单比特逻辑与运算和 4 个单比特逻辑异或运算，迭代 4 轮后密码性质可达到差分均匀度为 16、非线性度为 96，分量函数的代数次数能达到 6 且整体平衡。NUX[7]直接使用 4 个 4 bit 置换并置合成 16 bit S 盒，这种构造方式适合轻量级密码设计，但不能提高 S 盒的密码学性质。第二种情形是基于 SPS 结构构造。Piccolo 算法[8]采用了 SPS 结构构造的 16 bit S 盒，其中，小规模 S 盒为 4 bit，线性层为 4×4 的有限域 $F_2^4$ 上的极大距离可分（MDS, maximum distance separable）矩阵，但是 MDS 矩阵硬件实现占用资源多。第三种情形是基于非线性反馈移位寄存器（NFSR, nonlinear feedback shift register）直接构造，如 CACR2019 密码学会商用密码征集算法中 NBC 算法[9]基于 16 级非线性移位寄存器构造的 16 bit S 盒，以及 SPRING 算法[10]中 4 个 8 bit 寄存器互相反馈的环状串联结构构造的 32 bit S 盒，但是这 2 种方式构造的大规模 S 盒分别需要迭代 20 轮或 32 轮，硬件实现时延较大，而且 32 bit S 盒目前仍难以完全刻画其差分均匀度和非线性度等密码性质。美国国家标准与技术研究院（NIST）发起轻量级密码算法公开征集[11]，最终入围算法中 SPARKLE[12]及 GIFT-COFB（combined feedback）[13]等算法均采用了 32 bit 或者 64 bit 大规模密码 S 盒。第四种情形是基于 ARX 结构构造的大规模 S 盒，2020 年美洲密码会上，Christof 等[14]基于 ARX 结构构造了 64 bit S 盒 Alzette，仅使用循环移位、异或及模 $2^{32}$ 加基于 4 轮平衡 Feistel 结构构造 64 bit S 盒，在现代 CPU 上仅需 12 条指令迭代两次就可达到与 AES 一样安全，不过由于 64 bit S 盒规模较大，其密码学性质不易刻画。因此，大规模 S 盒构造不仅要合理选择密码结构，而且对 S 盒的尺寸也有要求，即至少能有效刻画其密码学性质。

基于 SPS 结构大规模 S 盒的构造主要体现在线性扩散层 $P$ 置换的设计上，$P$ 置换安全性设计指标主要是分支数，分支数反映了扩散变换的好坏，分支数越大，扩散变换效果越好。分支数与差分分析、线性分析密切相关，利用 $P$ 置换的分支数，评估活跃 S 盒数目的下界，从而量化分组密码抵抗差分分析和线性分析的能力。近些年，分组密码扩散层的研究成果非常丰富，主要有以下三类。1) 利用 MDS 码构造最优扩散层。基于线性变换与线性码的联系，寻找较大分支数的线性变换，也就是寻找距离较大的线性码，极大距离可分码的分支数达到了最大值，其对应的 MDS 矩阵是扩散层构造的较好选择，AES[15]、FOX[3]等分组密码都采用了 MDS 扩散层。2) 利用 MDBL（maximum distance binary linear）码构造最优扩散层。MDBL 矩阵的分支数是二元域矩阵所能取到的最大可能值，与 MDS 矩阵相比，MDBL 矩阵的扩散速度略慢，但由于不涉及有限域上的乘法，其硬件实现通常更加轻量化，而且 MDBL 矩阵更加灵活，更易于适应各种平台的优化实现，uBlock 分组密码[16]采用了 MDBL 扩散层。3) 利用具有良好数学性质的循环矩阵构造最优扩散层[17-18]。基于循环矩阵的构造策略被分组密码广泛采用，在循环矩阵中，任意行向量的每个元素都是前一行向量的各个元素依次右移一个位置的结果，从而使硬件实现复用乘法电路以节省硬件面积，利用循环矩阵可以非常灵活地在硬件面积和实现时延间进行折中。

基于 SPS 结构构造的大规模 S 盒作为分组密码算法的非线性核心部件，不仅大幅提高了算法抵抗差分/线性密码分析的攻击能力，而且给算法整体结构采取何种性质的线性变换留下了很大的选择空间。Donut[19]使用 4 个 8 bit 置换基于 SPS 结构构造 32 bit 大规模 S 盒，线性变换 $P$ 是基于 4×4 有限域 $F_2^8$ 上的 MDS 矩阵；Saturnin[20]使用 4 个 4 bit 置换基于 SPS 结构构造 16 bit 大规模 S 盒，4 bit 置换为最佳置换，线性变换 $P$ 为 4×4 有限域 $F_2^4$ 上的 MDS 矩阵。但是，由于有限域上 MDS 矩阵乘法运算的存在，硬件实现面积较大，导致传统 MDS 不适用于射频识别（RFID）系统和传感器网络等资源受限的环境。为了解决这一问题，Sajadieh 等[21]基于线性反馈移位寄存器（LFSR）提出了迭代型 MDS 矩阵扩散层的构造方式，在保证最优分支数的前提下，极大地节省了硬件实现面积。Wu 等[22]将矩阵元素

扩充到多项式环上，利用不同类型的 LFSR 结构设计轻量级最优扩散层。Augot 等[23]通过分析迭代矩阵的穷举搜索结果，结合 BCH 码相关结论，提出了最优迭代扩散层的直接构造算法。除硬件实现面积之外，时延也是扩散层设计的一个重要参数。Li 等[24-25]研究了低时延迭代型 MDS 矩阵和对合 MDS 矩阵的构造。Guo 等[26-27]通过提取矩阵可逆的充要条件以及分支数等价的划分原则，刻画了逆矩阵的具体形式和基本特征，提出了循环移位异或型最优扩散层的构造算法。文献[28]提出一种利用线性变换输入与输出关系反证得出分支数大小的普适方法，证明了一类由循环移位与异或运算构造的轻量级扩散变换是最优线性变换。

本文借鉴文献[28]线性变换输入输出关系反证法的思想，提出将最优线性变换目标问题转化为若干个递进关系定理的证明方法，不仅解决了该类最优线性变换的证明，而且适用于任意线性变换的证明，并在此基础上研究了 2 轮 SPS 结构的大规模 S 盒构造问题。本文主要贡献如下：基于循环移位与异或运算构造了有限域上分支数最佳的线性变换 $P$，给出了该类最优线性变换的一种新的证明方法，建立了 2 轮 SPS 结构的大规模 S 盒模型，通过小规模 S 盒与最优循环移位–异或型矩阵，设计了一系列密码学性质优良的轻量级大规模 S 盒，与已有大规模 S 盒构造方法相比，本文的大规模 S 盒设计方案运算代价更加低廉，其差分、线性等密码学性质更加优良。

## 1　基本概念及引理

**定义 1**[29]　设 $f$ 是一个 $F_2^n \to F_2^n$ 的函数，对任意输入差分和输出差分 $\Delta \boldsymbol{x}, \Delta \boldsymbol{y} \in F_2^n$，任意输入掩码和输出掩码 $\boldsymbol{w}, \boldsymbol{v} \in F_2^n$，差分概率和线性概率分别定义为

$$\mathrm{DP}^f(\Delta \boldsymbol{x} \to \Delta \boldsymbol{y}) = \frac{\#\{\boldsymbol{x} \in F_2^n \mid f(\boldsymbol{x} \oplus \Delta \boldsymbol{x}) \oplus f(\boldsymbol{x}) = \Delta \boldsymbol{y}\}}{2^n}$$

$$\mathrm{LP}^f(\boldsymbol{w} \to \boldsymbol{v}) = \left( \frac{\#\{\boldsymbol{x} \in F_2^n \mid \boldsymbol{v} f(\boldsymbol{x}) = \boldsymbol{w} \boldsymbol{x}\}}{2^{n-1}} - 1 \right)^2$$

**定义 2**[29]　设 $f$ 为 S 盒，记其最大差分概率和线性概率分别为

$$p = \max_{\Delta \boldsymbol{x} \neq \boldsymbol{0}, \Delta \boldsymbol{y}} \mathrm{DP}^S(\Delta \boldsymbol{x} \to \Delta \boldsymbol{y})$$

$$q = \max_{\boldsymbol{v} \neq \boldsymbol{0}, \boldsymbol{w}} \mathrm{LP}^S(\boldsymbol{w} \to \boldsymbol{v})$$

**定义 3**[9]　设 $f$ 是一个 $F_2^n \to F_2^n$ 的函数，对任意输入差分和输出差分 $\Delta \boldsymbol{x}, \Delta \boldsymbol{y} \in F_2^n$，任意输入掩码和输出掩码 $\boldsymbol{w}, \boldsymbol{v} \in F_2^n$，差分均匀度和线性度分别定义为

$$\mathrm{Diff}(f) = \max_{\substack{\boldsymbol{0} \neq \Delta \boldsymbol{x} \in F_2^n \\ \Delta \boldsymbol{y} \in F_2^n}} \#\left\{ \boldsymbol{x} \in F_2^n : f(\boldsymbol{x} \oplus \Delta \boldsymbol{x}) \oplus S(\boldsymbol{x}) = \Delta \boldsymbol{y} \right\}$$

$$\mathrm{Lin}(f) = \max_{\substack{\boldsymbol{w} \in F_2^n \\ \boldsymbol{0} \neq \boldsymbol{v} \in F_2^n}} \left| \#\left\{ \boldsymbol{x} \in F_2^n : \boldsymbol{v} f(\boldsymbol{x}) = \boldsymbol{w} \boldsymbol{x} \right\} - \# \right.$$

$$\left. \left\{ \boldsymbol{x} \in F_2^n : \boldsymbol{v} f(\boldsymbol{x}) \neq \boldsymbol{w} \boldsymbol{x} \right\} \right|$$

**定义 4**[28]　对于扩散层的输入 $\boldsymbol{X} = (x_1, x_2, \cdots, x_m) \in (F_2^n)^m$，$W(\boldsymbol{X})$ 定义为 $x_1, x_2, \cdots, x_m$ 中非 0 的个数，即 $W(\boldsymbol{X}) = \left| \{ x_i, x_i \neq 0, 1 \leqslant i \leqslant m \} \right|$。

**定义 5**[28]　设 $P(\boldsymbol{X})$ 是一个 $(F_2^n)^m \to (F_2^n)^m$ 上的置换，输入 $\boldsymbol{X} = (x_1, x_2, \cdots, x_m) \in (F_2^n)^m$，则扩散层 $P$ 的分支数定义为 $B_d(P) = \min_{\boldsymbol{X} \neq \boldsymbol{0}} \{ W(\boldsymbol{X}) + W(P(\boldsymbol{X})) \}$。

当 $B_d(P) = m + 1$ 时，扩散层的分支数达到最大，被称为最优线性变换[12]。

**定义 6**[27]　令 $n$ 和 $b$ 是 2 个正整数，$I \subset \{0, 1, \cdots, nb - 1\}$，称 $\boldsymbol{M}_{n,b}^I$ 是 $(F_2^b)^n$ 上由 $I$ 决定的循环移位–异或型线性扩散层，记 $\boldsymbol{M}_{n,b}^I \boldsymbol{x} = \bigoplus_{i \in I} (\boldsymbol{x} <<< i)$，其中，$\boldsymbol{x}$ 是 $nb$ bit 的输入向量。

设 $\boldsymbol{M}_{4,b}^I$ 是一个比特循环矩阵，可以将 $\boldsymbol{M}_{4,b}^I$ 表示为

$$\mathrm{Circ}(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}) = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B} & \boldsymbol{C} & \boldsymbol{D} \\ \boldsymbol{D} & \boldsymbol{A} & \boldsymbol{B} & \boldsymbol{C} \\ \boldsymbol{C} & \boldsymbol{D} & \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{B} & \boldsymbol{C} & \boldsymbol{D} & \boldsymbol{A} \end{bmatrix}$$

其中，$\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$ 和 $\boldsymbol{D}$ 均为 $F_2$ 上的 $b \times b$ 矩阵。

对任意的集合 $I$，假设 $\boldsymbol{M}_{4,b}^I$ 是一个 MDS 矩阵，则该矩阵的分支数记为 $B_d(\boldsymbol{M}_{4,b}^I)$。

很明显，若 $\boldsymbol{M}_{4,b}^I$ 是一个 MDS 矩阵，则 $B_d(\boldsymbol{M}_{4,b}^I) = 5$。

**定义 7**[30]　对于 2 个 $n \times n$ 阶二元矩阵 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$，如果存在一个行置换 $\rho$ 和一个列置换 $\gamma$，满足 $\rho(\gamma(\boldsymbol{P})) = \gamma(\rho(\boldsymbol{Q})) = \boldsymbol{Q}$，则称 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 为置换同形矩阵。

**引理 1**[30]　若 2 个 $n \times n$ 阶二元矩阵 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 是置换同形的，则 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 具有相同的分支数，即 $B_d(\boldsymbol{P}) = B_d(\boldsymbol{Q})$。

**性质 1**　设 $\boldsymbol{M}_{4,b}^I$ 是一个循环移位–异或型矩阵，其中，$I = \{i_1, \cdots, i_5\}$ 且 $0 \leqslant i_1 < \cdots < i_5 \leqslant 4b - 1$，那么一定存在 $I' = \{(i_1 + b) \bmod 4b, \cdots, (i_5 + b) \bmod 4b\}$ 的另一个矩阵 $\boldsymbol{M}_{4,b}^{I'}$，使 $B_d(\boldsymbol{M}_{4,b}^I) = B_d(\boldsymbol{M}_{4,b}^{I'})$。

**证明**　若 $\boldsymbol{M}_{4,b}^{I}\boldsymbol{x}=\underset{i\in I}{\oplus}(\boldsymbol{x}<<<i)$，则 $\boldsymbol{M}_{4,b}^{I'}\boldsymbol{x}=\underset{i\in I'}{\oplus}(\boldsymbol{x}<<<i)=\underset{i\in I+b}{\oplus}(\boldsymbol{x}<<<i)$。记

$$\boldsymbol{M}_{4,b}^{I}=\mathrm{Circ}(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D})=\begin{bmatrix}\boldsymbol{A}&\boldsymbol{B}&\boldsymbol{C}&\boldsymbol{D}\\ \boldsymbol{D}&\boldsymbol{A}&\boldsymbol{B}&\boldsymbol{C}\\ \boldsymbol{C}&\boldsymbol{D}&\boldsymbol{A}&\boldsymbol{B}\\ \boldsymbol{B}&\boldsymbol{C}&\boldsymbol{D}&\boldsymbol{A}\end{bmatrix}$$

$$\boldsymbol{M}_{4,b}^{I'}=\mathrm{Circ}(\boldsymbol{D},\boldsymbol{A},\boldsymbol{B},\boldsymbol{C})=\begin{bmatrix}\boldsymbol{D}&\boldsymbol{A}&\boldsymbol{B}&\boldsymbol{C}\\ \boldsymbol{C}&\boldsymbol{D}&\boldsymbol{A}&\boldsymbol{B}\\ \boldsymbol{B}&\boldsymbol{C}&\boldsymbol{D}&\boldsymbol{A}\\ \boldsymbol{A}&\boldsymbol{B}&\boldsymbol{C}&\boldsymbol{D}\end{bmatrix}$$

由引理 1 可知，存在一个行向量线性变换 $\sigma=\sigma_1\sigma_2\sigma_3$，使 $\boldsymbol{M}_{4,b}^{I'}\sigma=\boldsymbol{M}_{4,b}^{I}$，其中 $\sigma_3$ 表示矩阵 $\boldsymbol{M}_{4,b}^{I'}$ 的第 4 行与第 3 行互换，$\sigma_2$ 表示第 3 行与第 2 行互换，$\sigma_1$ 表示第 2 行与第 1 行互换。所以 $B_d(\boldsymbol{M}_{4,b}^{I})=B_d(\boldsymbol{M}_{4,b}^{I'})$。

**性质 2**　设 $\boldsymbol{M}_{4,b}^{I}$ 是一个循环移位–异或型矩阵，其中，$I=\{i_1,\cdots,i_5\}$ 且 $0\leqslant i_1<\cdots<i_5\leqslant 4b-1$，那么一定存在 $I'=\{(4b-i_1)\bmod 4b,\cdots,(4b-i_5)\bmod 4b\}$ 的另一矩阵 $\boldsymbol{M}_{4,b}^{I'}$，使 $B_d(\boldsymbol{M}_{4,b}^{I})=B_d(\boldsymbol{M}_{4,b}^{I'})$。

**证明**　由于

$$\boldsymbol{M}_{4,b}^{I}\boldsymbol{x}=\underset{i\in I}{\oplus}(\boldsymbol{x}<<<i)=\underset{i\in I}{\oplus}(\boldsymbol{x}>>>(4b-i))$$

$$\boldsymbol{M}_{4,b}^{I'}\boldsymbol{x}=\underset{i\in 4b-I}{\oplus}(\boldsymbol{x}<<<i)=\underset{i\in 4b-I}{\oplus}(\boldsymbol{x}>>>(4b-i))$$

$$\boldsymbol{M}_{4,b}^{I}=\mathrm{Circ}(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D})=\begin{bmatrix}\boldsymbol{A}&\boldsymbol{B}&\boldsymbol{C}&\boldsymbol{D}\\ \boldsymbol{D}&\boldsymbol{A}&\boldsymbol{B}&\boldsymbol{C}\\ \boldsymbol{C}&\boldsymbol{D}&\boldsymbol{A}&\boldsymbol{B}\\ \boldsymbol{B}&\boldsymbol{C}&\boldsymbol{D}&\boldsymbol{A}\end{bmatrix}$$

$$\boldsymbol{M}_{4,b}^{I'}=\mathrm{Circ}(\boldsymbol{B},\boldsymbol{C},\boldsymbol{D},\boldsymbol{A})=\begin{bmatrix}\boldsymbol{B}&\boldsymbol{C}&\boldsymbol{D}&\boldsymbol{A}\\ \boldsymbol{C}&\boldsymbol{D}&\boldsymbol{A}&\boldsymbol{B}\\ \boldsymbol{D}&\boldsymbol{A}&\boldsymbol{B}&\boldsymbol{C}\\ \boldsymbol{A}&\boldsymbol{B}&\boldsymbol{C}&\boldsymbol{D}\end{bmatrix}$$

由引理 1 可知，存在一个行向量线性变换 $\sigma=\sigma_1\sigma_2$，使 $\boldsymbol{M}_{4,b}^{I'}\sigma=M_{4,b}^{I}$，其中 $\sigma_2$ 表示矩阵 $\boldsymbol{M}_{4,b}^{I'}$ 的第 4 行与第 1 行互换，$\sigma_1$ 表示第 3 行与第 2 行互换。所以 $B_d(\boldsymbol{M}_{4,b}^{I})=B_d(\boldsymbol{M}_{4,b}^{I'})$。证毕。

**引理 2**[29]　假设分组密码算法轮密钥是随机独立均匀分布的，且与每轮的输入数据按照逐比特异或运算。若线性扩散层的分支数为 $d$，小部件 S 盒的最大差分概率为 $p$，则 SPS 结构函数差分概率的上界为 $p^{d-1}$。

**引理 3**[29]　假设分组密码算法轮密钥是随机独立均匀分布的，且与每轮的输入数据按照逐比特异或运算。若线性扩散层的分支数为 $d$，小部件 S 盒的最大线性概率为 $q$，则 SPS 结构函数线性概率的上界为 $q^{d-1}$。

**定义 8**　一般形式。设 $\boldsymbol{X}\in(F_2^n)^m$，定义基于循环移位与异或运算的线性变换为

$$L(\boldsymbol{X},m,n)=(\boldsymbol{X}<<<l_1)\oplus(\boldsymbol{X}<<<l_2)\oplus\cdots\oplus(\boldsymbol{X}<<<l_r)$$

其中，$0\leqslant l_i<l_{i+1}<nm$，$1\leqslant r\leqslant nm$。

**引理 4**[31]　线性变换 $L(\boldsymbol{X},m,n)$ 是最优线性变换必须满足以下 2 个必要条件。

1) $r$ 为奇数且 $r\geqslant m$。

2) 至少存在 $m$ 个 $l_i$，满足 $ni\leqslant l_i<n(i+1)$，$i=0,1,\cdots,m-1$。

## 2　一类最优循环移位–异或型线性变换的证明

本节根据第 1 节给出的一般形式和必要条件，讨论最简形式下的最优循环移位–异或型线性变换，即最优线性变换中循环移位项数最少的形式。本节给出了输入为 $(F_2^n)^4$ 扩散层中最简形式下的最优线性变换，并对其中一种进行了详细证明。

**定理 1**　若 $(F_2^n)^4\to(F_2^n)^4$ 上基于循环移位–异或型扩散结构，即

$$\boldsymbol{A}\to\boldsymbol{B}:\boldsymbol{B}=\boldsymbol{A}\oplus(\boldsymbol{A}<<<n)\oplus(\boldsymbol{A}<<<(n+t))\oplus(\boldsymbol{A}<<<(2n+t))\oplus(\boldsymbol{A}<<<(3n+t))$$

其中，$n$ 是 4 的倍数，$t=\dfrac{n}{4}$。设 $\boldsymbol{A}=(a_0,a_1,a_2,a_3)$，$\boldsymbol{B}=(b_0,b_1,b_2,b_3)$，$a_i,b_i\,(0\leqslant i\leqslant 3)\in F_2^n$，则

$$\begin{aligned}b_0&=a_0\oplus a_1\oplus((a_1\oplus a_2\oplus a_3)<<t)\oplus((a_0\oplus a_2\oplus a_3)>>(n-t))\\ b_1&=a_1\oplus a_2\oplus((a_0\oplus a_2\oplus a_3)<<t)\oplus((a_0\oplus a_1\oplus a_3)>>(n-t))\\ b_2&=a_2\oplus a_3\oplus((a_0\oplus a_1\oplus a_3)<<t)\oplus((a_0\oplus a_1\oplus a_2)>>(n-t))\\ b_3&=a_3\oplus a_0\oplus((a_0\oplus a_1\oplus a_2)<<t)\oplus((a_1\oplus a_2\oplus a_3)>>(n-t))\end{aligned}$$

**证明**　由于 $\boldsymbol{A}\in(F_2^n)^4$，$n$ 是 4 的倍数，$t=\dfrac{n}{4}$，且

$$\boldsymbol{A}=(a_0,a_1,a_2,a_3)\tag{1}$$

$$\boldsymbol{A}<<<n=(a_1,a_2,a_3,a_0)\tag{2}$$

$$\boldsymbol{A} <<< (n+t) = ((\boldsymbol{A} <<< n) <<< t) \tag{3}$$

$$\boldsymbol{A} <<< (2n+t) = ((\boldsymbol{A} <<< 2n) <<< t) \tag{4}$$

$$\boldsymbol{A} <<< (3n+t) = ((\boldsymbol{A} <<< 3n) <<< t) \tag{5}$$

由式(3)～式(5)可得

$$(\boldsymbol{A} <<< (n+t)) \oplus (\boldsymbol{A} <<< (2n+t)) \oplus (\boldsymbol{A} <<< (3n+t)) =$$
$$((\boldsymbol{A} <<< n) <<< t) \oplus ((\boldsymbol{A} <<< 2n) <<< t) \oplus$$
$$((\boldsymbol{A} <<< 3n) <<< t) = ((\boldsymbol{A} <<< n) \oplus (\boldsymbol{A} <<< 2n) \oplus$$
$$(\boldsymbol{A} <<< 3n)) <<< t = ((a_1, a_2, a_3, a_0) \oplus (a_2, a_3, a_0, a_1) \oplus$$
$$(a_3, a_0, a_1, a_2)) <<< t = (a_1 \oplus a_2 \oplus a_3, a_2 \oplus a_3 \oplus a_0, a_3 \oplus$$
$$a_0 \oplus a_1, a_0 \oplus a_1 \oplus a_2) <<< t =$$
$$(((a_1 \oplus a_2 \oplus a_3) << t) \oplus ((a_0 \oplus a_2 \oplus a_3) >> (n-t)),$$
$$((a_0 \oplus a_2 \oplus a_3) << t) \oplus ((a_0 \oplus a_1 \oplus a_3) >> (n-t)),$$
$$((a_0 \oplus a_1 \oplus a_3) << t) \oplus ((a_0 \oplus a_1 \oplus a_2) >> (n-t)),$$
$$((a_0 \oplus a_1 \oplus a_2) << t) \oplus ((a_1 \oplus a_2 \oplus a_3) >> (n-t)))$$

所以，由

$$\boldsymbol{B} = \boldsymbol{A} \oplus (\boldsymbol{A} <<< n) \oplus (\boldsymbol{A} <<< (n+t)) \oplus$$
$$(\boldsymbol{A} <<< (2n+t)) \oplus (\boldsymbol{A} <<< (3n+t))$$

可得

$$\boldsymbol{B} = \boldsymbol{A} \oplus (\boldsymbol{A} <<< n) \oplus ((\boldsymbol{A} <<< n) \oplus$$
$$(\boldsymbol{A} <<< 2n) \oplus (\boldsymbol{A} <<< 3n)) <<< t$$

$$b_0 = a_0 \oplus a_1 \oplus ((a_1 \oplus a_2 \oplus a_3) << t) \oplus$$
$$((a_0 \oplus a_2 \oplus a_3) >> (n-t))$$

$$b_1 = a_1 \oplus a_2 \oplus ((a_0 \oplus a_2 \oplus a_3) << t) \oplus$$
$$((a_0 \oplus a_1 \oplus a_3) >> (n-t))$$

$$b_2 = a_2 \oplus a_3 \oplus ((a_0 \oplus a_1 \oplus a_3) << t) \oplus$$
$$((a_0 \oplus a_1 \oplus a_2) >> (n-t))$$

$$b_3 = a_3 \oplus a_0 \oplus ((a_0 \oplus a_1 \oplus a_2) << t) \oplus$$
$$((a_1 \oplus a_2 \oplus a_3) >> (n-t))$$

证毕。

**定理 2**　设 $n$ 是 4 的倍数，$t = \frac{n}{4}$，$a_0 \in F_2^n$，$a_0 \neq 0$。令

$$b_0 = a_0 \oplus (a_0 >> (n-t))$$

$$b_1 = b_2 = (a_0 << t) \oplus (a_0 >> (n-t))$$

$$b_3 = a_0 \oplus (a_0 << t)$$

则 $b_0, b_1, b_2, b_3$ 都不为 0。

**证明**　使用反证法。只证 $b_3 \neq 0$，其他类似可证。设 $a_0 = (a_{00}, a_{01}, a_{02}, a_{03}), a_{0i} (0 \leqslant i \leqslant 3) \in F_2^t$，则 $a_0 << t = (a_{01}, a_{02}, a_{03}, 0)$，从而 $b_3 = (a_{00} \oplus a_{01}, a_{01} \oplus a_{02}, a_{02} \oplus a_{03}, a_{03})$。若 $b_3$ 为 0，则 $a_{00} \oplus a_{01} = a_{01} \oplus a_{02} = a_{02} \oplus a_{03} = a_{03} = 0$，从而 $a_{03} = a_{02} = a_{01} = a_{00} = 0$，即 $a_0 = 0$，与条件 $a_0 \neq 0$ 矛盾，故 $b_3 \neq 0$。证毕。

**定理 3**　设 $n$ 是 4 的倍数，$t = \frac{n}{4}$，$a_0, a_1 \in F_2^n$，$a_0, a_1 \neq 0$。令

$$b_0 = a_0 \oplus a_1 \oplus (a_1 << t) \oplus (a_0 >> (n-t))$$
$$b_1 = a_1 \oplus (a_0 << t) \oplus ((a_0 \oplus a_1) >> (n-t))$$
$$b_2 = ((a_0 \oplus a_1) << t) \oplus ((a_0 \oplus a_1) >> (n-t))$$
$$b_3 = a_0 \oplus ((a_0 \oplus a_1) << t) \oplus (a_1 >> (n-t))$$

则 $a_0 = a_1$ 时，$b_0, b_1, b_3$ 都不为 0；$a_0 \neq a_1$ 时，$b_0, b_1, b_3$ 中至少有 2 个不为 0，且 $b_2 \neq 0$。

**证明**

1) $a_0 = a_1$ 时，$b_0 = (a_0 << t) \oplus (a_0 >> (n-t))$，$b_1 = a_0 \oplus (a_0 << t)$，$b_2 = 0$，$b_3 = a_0 \oplus (a_0 >> (n-t))$。由定理 2 可知，$b_0, b_1, b_3$ 都不为 0。

2) $a_0 \neq a_1$ 时，由于 $b_0 \oplus b_1 \oplus b_3 = 0$，从而只需证明 $b_0, b_1, b_3$ 不全为 0 即可。设 $a_i = (a_{i0}, a_{i1}, a_{i2}, a_{i3}), a_{ij} (0 \leqslant i \leqslant 1, 0 \leqslant j \leqslant 3) \in F_2^t$，则

$$a_1 << t = (a_{11}, a_{12}, a_{13}, 0)$$
$$a_0 >> (n-t) = (0, 0, 0, a_{00})$$
$$a_0 << t = (a_{01}, a_{02}, a_{03}, 0)$$
$$(a_0 \oplus a_1) >> (n-t) = (0, 0, 0, a_{00} \oplus a_{10})$$
$$(a_0 \oplus a_1) << t = (a_{01} \oplus a_{11}, a_{02} \oplus a_{12}, a_{03} \oplus a_{13}, 0)$$
$$a_1 >> (n-t) = (0, 0, 0, a_{10})$$

从而

$$b_0 = (a_{00} \oplus a_{10} \oplus a_{11}, a_{01} \oplus a_{11} \oplus a_{12},$$
$$a_{02} \oplus a_{12} \oplus a_{13}, a_{03} \oplus a_{13} \oplus a_{00})$$
$$b_1 = (a_{10} \oplus a_{01}, a_{11} \oplus a_{02}, a_{12} \oplus a_{03}, a_{13} \oplus a_{00} \oplus a_{10})$$
$$b_2 = (a_{01} \oplus a_{11}, a_{02} \oplus a_{12}, a_{03} \oplus a_{13}, a_{00} \oplus a_{10})$$
$$b_3 = (a_{00} \oplus a_{01} \oplus a_{11}, a_{01} \oplus a_{02} \oplus a_{12}, a_{02} \oplus$$
$$a_{03} \oplus a_{13}, a_{03} \oplus a_{10})$$

若 $b_0 = b_1 = b_3 = 0$，则

$$a_{00} \oplus a_{10} \oplus a_{11} = a_{01} \oplus a_{11} \oplus a_{12} = a_{02} \oplus a_{12} \oplus a_{13} = 0$$
$$a_{03} \oplus a_{13} \oplus a_{00} = a_{10} \oplus a_{01} = a_{11} \oplus a_{02} = 0$$
$$a_{12} \oplus a_{03} = a_{13} \oplus a_{00} \oplus a_{10} = a_{00} \oplus a_{01} \oplus a_{11} = 0$$
$$a_{01} \oplus a_{02} \oplus a_{12} = a_{02} \oplus a_{03} \oplus a_{13} = a_{03} \oplus a_{10} = 0$$

从而 $a_{00}=a_{01}=a_{02}=a_{03}=a_{10}=a_{11}=a_{12}=a_{13}=0$，即 $a_0=a_1=0$，与条件 $a_0,a_1\neq 0$ 矛盾，故 $b_0,b_1,b_3$ 不全为 0，即 $b_0,b_1,b_3$ 中至少有 2 个不为 0。

若 $b_2=0$，则 $a_{01}\oplus a_{11}=a_{02}\oplus a_{12}=a_{03}\oplus a_{13}=a_{00}\oplus a_{10}=0$，即 $a_0=a_1$，与条件 $a_0\neq a_1$ 矛盾。

所以 $b_2\neq 0$。证毕。

**定理 4** 设 $n$ 是 4 的倍数，$t=\dfrac{n}{4}$，$a_0,a_1,a_2\in F_2^n$，$a_0,a_1,a_2\neq 0$，令

$$b_0=a_0\oplus a_1\oplus((a_1\oplus a_2)<<t)\oplus((a_0\oplus a_2)>>(n-t))$$

$$b_1=a_1\oplus a_2\oplus((a_0\oplus a_2)<<t)\oplus((a_0\oplus a_1)>>(n-t))$$

$$b_2=a_2\oplus((a_0\oplus a_1)<<t)\oplus((a_0\oplus a_1\oplus a_2)>>(n-t))$$

$$b_3=a_0\oplus((a_0\oplus a_1\oplus a_2)<<t)\oplus((a_1\oplus a_2)>>(n-t))$$

则 $b_0,b_1,b_2,b_3$ 中至少有 2 个不为 0。

**证明** 由于

$$b_0\oplus b_1\oplus b_3=a_2\oplus(a_2<<t)$$

$$b_0\oplus b_1\oplus b_2=a_0\oplus(a_0>>(n-t))$$

$$b_0\oplus b_2\oplus b_3=(a_1\oplus a_2)\oplus(a_1<<t)\oplus(a_2>>(n-t))$$

$$b_1\oplus b_2\oplus b_3=(a_0\oplus a_1)\oplus(a_0<<t)\oplus(a_1>>(n-t))$$

因为 $a_0,a_2\neq 0$，由定理 2 可知，$b_0\oplus b_1\oplus b_3$ 和 $b_0\oplus b_1\oplus b_2$ 都不为 0。

1) 当 $b_2\neq 0$ 时，由 $b_0\oplus b_1\oplus b_3\neq 0$ 可知，$b_0,b_1,b_3$ 中至少有一个不为 0，从而 $b_0,b_1,b_2,b_3$ 中至少有 2 个不为 0。

2) 当 $b_3\neq 0$ 时，由 $b_0\oplus b_1\oplus b_2\neq 0$ 可知，$b_0,b_1,b_2$ 中至少有一个不为 0，从而 $b_0,b_1,b_2,b_3$ 中至少有 2 个不为 0。

3) 当 $b_2=0$ 且 $b_3=0$ 时，以下证明 $b_0\neq 0$ 和 $b_1\neq 0$。设

$$a_i=(a_{i0},a_{i1},a_{i2},a_{i3}),a_{ij}(0\leqslant i\leqslant 2,0\leqslant j\leqslant 3)\in F_2^t$$

则

$$(a_1\oplus a_2)<<t=(a_{11}\oplus a_{21},a_{12}\oplus a_{22},a_{13}\oplus a_{23},0)$$

$$(a_0\oplus a_2)>>(n-t)=(0,0,0,a_{00}\oplus a_{20})$$

$$(a_0\oplus a_2)<<t=(a_{01}\oplus a_{21},a_{02}\oplus a_{22},a_{03}\oplus a_{23},0)$$

$$(a_0\oplus a_1)>>(n-t)=(0,0,0,a_{00}\oplus a_{10})$$

$$(a_0\oplus a_1)<<t=(a_{01}\oplus a_{11},a_{02}\oplus a_{12},a_{03}\oplus a_{13},0)$$

$$(a_0\oplus a_1\oplus a_2)>>(n-t)=(0,0,0,a_{00}\oplus a_{10}\oplus a_{20})$$

$$(a_0\oplus a_1\oplus a_2)<<t=$$
$$(a_{01}\oplus a_{11}\oplus a_{21},a_{02}\oplus a_{12}\oplus a_{22},a_{03}\oplus a_{13}\oplus a_{23},0)$$

$$(a_1\oplus a_2)>>(n-t)=(0,0,0,a_{10}\oplus a_{20})$$

从而

$$b_0=(a_{00}\oplus a_{10}\oplus a_{11}\oplus a_{21},a_{01}\oplus a_{11}\oplus a_{12}\oplus a_{22},$$
$$a_{02}\oplus a_{12}\oplus a_{13}\oplus a_{23},a_{03}\oplus a_{13}\oplus a_{00}\oplus a_{20})$$

$$b_1=(a_{10}\oplus a_{20}\oplus a_{01}\oplus a_{21},a_{11}\oplus a_{21}\oplus a_{02}\oplus a_{22},$$
$$a_{12}\oplus a_{22}\oplus a_{03}\oplus a_{23},a_{13}\oplus a_{23}\oplus a_{00}\oplus a_{10})$$

$$b_2=(a_{20}\oplus a_{01}\oplus a_{11},a_{21}\oplus a_{02}\oplus a_{12},a_{22}\oplus a_{03}\oplus a_{13},$$
$$a_{23}\oplus a_{00}\oplus a_{10}\oplus a_{20})$$

$$b_3=(a_{00}\oplus a_{01}\oplus a_{11}\oplus a_{21},a_{01}\oplus a_{02}\oplus a_{12}\oplus a_{22},$$
$$a_{02}\oplus a_{03}\oplus a_{13}\oplus a_{23},a_{03}\oplus a_{10}\oplus a_{20})$$

①若 $b_0=0$，则 $b_0=b_2=b_3=0$，即

$$a_{00}\oplus a_{10}\oplus a_{11}\oplus a_{21}=a_{01}\oplus a_{11}\oplus a_{12}\oplus a_{22}=$$
$$a_{02}\oplus a_{12}\oplus a_{13}\oplus a_{23}=a_{03}\oplus a_{13}\oplus a_{00}\oplus a_{20}=$$
$$a_{20}\oplus a_{01}\oplus a_{11}=a_{21}\oplus a_{02}\oplus a_{12}=$$
$$a_{22}\oplus a_{03}\oplus a_{13}=a_{23}\oplus a_{00}\oplus a_{10}\oplus a_{20}=$$
$$a_{00}\oplus a_{01}\oplus a_{11}\oplus a_{21}=a_{01}\oplus a_{02}\oplus a_{12}\oplus a_{22}=$$
$$a_{02}\oplus a_{03}\oplus a_{13}\oplus a_{23}=a_{03}\oplus a_{10}\oplus a_{20}=0$$

从而 $a_{00}=a_{01}=a_{02}=a_{03}=0$，即 $a_0=0$，与条件 $a_0\neq 0$ 矛盾，故 $b_0\neq 0$。

②若 $b_1=0$，则 $b_1=b_2=b_3=0$，与①同理可得 $a_0=0$，与条件 $a_0\neq 0$ 矛盾，故 $b_1\neq 0$。

由①和②知，$b_0$ 和 $b_1$ 都不为 0，从而 $b_0,b_1,b_2,b_3$ 中至少有 2 个不为 0。证毕。

**定理 5** 设 $n$ 是 4 的倍数，$t=\dfrac{n}{4}$，$a_0,a_1,a_2,a_3\in F_2^n$，$a_0,a_1,a_2,a_3\neq 0$，令

$$b_0=a_0\oplus a_1\oplus((a_1\oplus a_2\oplus a_3)<<t)\oplus((a_0\oplus a_2\oplus a_3)>>(n-t))$$

$$b_1=a_1\oplus a_2\oplus((a_0\oplus a_2\oplus a_3)<<t)\oplus((a_0\oplus a_1\oplus a_3)>>(n-t))$$

$$b_2=a_2\oplus a_3\oplus((a_0\oplus a_1\oplus a_3)<<t)\oplus((a_0\oplus a_1\oplus a_2)>>(n-t))$$

$$b_3=a_3\oplus a_0\oplus((a_0\oplus a_1\oplus a_2)<<t)\oplus((a_1\oplus a_2\oplus a_3)>>(n-t))$$

则 $b_0,b_1,b_2,b_3$ 中至少有一个不为 0。

**证明** 由于

$$b_0 \oplus b_1 \oplus b_2 \oplus b_3 = ((a_0 \oplus a_1 \oplus a_2 \oplus a_3) << t) \oplus ((a_0 \oplus a_1 \oplus a_2 \oplus a_3) >> (n-t))$$

1) 当 $a_0 \oplus a_1 \oplus a_2 \oplus a_3 \neq 0$ 时，由定理 2 可知，$b_0 \oplus b_1 \oplus b_2 \oplus b_3 \neq 0$，从而 $b_0, b_1, b_2, b_3$ 中至少有一个不为 0。

2) 当 $a_0 \oplus a_1 \oplus a_2 \oplus a_3 = 0$ 时，分 2 种情况讨论。

①若 $a_0 = a_1 = a_2 = a_3$，则 $b_0 = (a_0 << t) \oplus (a_0 >> (n-t))$，由定理 2 可知，$b_0 \neq 0$。

② 若 $a_0, a_1, a_2, a_3$ 不全相等，不妨设 $a_0 \oplus a_2 \neq 0$，则

$$b_0 \oplus b_2 = ((a_0 \oplus a_2) << t) \oplus ((a_0 \oplus a_2) >> (n-t))$$

由定理 2 可知，$b_0 \oplus b_2 \neq 0$。即 $b_0, b_2$ 至少有一个不为 0。

综上，$b_0, b_1, b_2, b_3$ 中至少有一个不为 0。证毕。

**定理 6**　设 $n$ 是 4 的倍数，$t = \frac{n}{4}$，$(F_2^n)^4 \to (F_2^n)^4$ 上基于循环移位–异或型线性变换

$$\boldsymbol{B} = L(\boldsymbol{A}) = \boldsymbol{A} \oplus (\boldsymbol{A} <<< n) \oplus (\boldsymbol{A} <<< (n+t)) \oplus (\boldsymbol{A} <<< (2n+t)) \oplus (\boldsymbol{A} <<< (3n+t))$$

则 $L$ 是一个最优线性变换。

**证明**　设

$$\boldsymbol{A} = (a_0, a_1, a_2, a_3), \boldsymbol{B} = (b_0, b_1, b_2, b_3)$$
$$a_i, b_i (0 \leqslant i \leqslant 3) \in F_2^n$$

则由定理 1 可得

$$b_0 = a_0 \oplus a_1 \oplus ((a_1 \oplus a_2 \oplus a_3) << t) \oplus ((a_0 \oplus a_2 \oplus a_3) >> (n-t)) \tag{6}$$

$$b_1 = a_1 \oplus a_2 \oplus ((a_0 \oplus a_2 \oplus a_3) << t) \oplus ((a_0 \oplus a_1 \oplus a_3) >> (n-t)) \tag{7}$$

$$b_2 = a_2 \oplus a_3 \oplus ((a_0 \oplus a_1 \oplus a_3) << t) \oplus ((a_0 \oplus a_1 \oplus a_2) >> (n-t)) \tag{8}$$

$$b_3 = a_3 \oplus a_0 \oplus ((a_0 \oplus a_1 \oplus a_2) << t) \oplus ((a_1 \oplus a_2 \oplus a_3) >> (n-t)) \tag{9}$$

需证明所有 $a_i, b_i (i = 0,1,2,3)$ 的非 0 个数之和不小于 5。下面分别讨论 $a_0, a_1, a_2, a_3$ 中至少有一个不为 0 情况下 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的非 0 个数之和，也就是 $\boldsymbol{A}$ 的非 0 个数分别为 1、2、3、4 时上述线性扩散变换的分支数。从式(6)～式(9)可以看到，$b_0, b_1, b_2, b_3$ 的形式相似，所以分类讨论时，从 $a_0, a_1, a_2, a_3$ 中任意选取 $a_i$ 不为 0 后会得到相似形式的 $b_0, b_1, b_2, b_3$，所以不同 $a_i$ 的选取对证明过程不会产生影响。

1) $a_0 \neq 0$ 且 $a_1 = a_2 = a_3 = 0$ 时，$b_0, b_1, b_2, b_3$ 都不为 0。事实上，$a_1 = a_2 = a_3 = 0$ 时，$b_0 = a_0 \oplus (a_0 >> (n-t))$，$b_1 = b_2 = (a_0 << t) \oplus (a_0 >> (n-t))$，$b_3 = a_0 \oplus (a_0 << t)$。

由定理 2 可知，$b_0, b_1, b_2, b_3$ 都不为 0。

2) $a_0, a_1 \neq 0$ 且 $a_2 = a_3 = 0$ 时，$b_0, b_1, b_2, b_3$ 中至少有 3 个不为 0。事实上，$a_2 = a_3 = 0$ 时，$b_0 = a_0 \oplus a_1 \oplus (a_1 << t) \oplus (a_0 >> (n-t))$，$b_1 = a_1 \oplus (a_0 << t) \oplus ((a_0 \oplus a_1) >> (n-t))$，$b_2 = ((a_0 \oplus a_1) << t) \oplus ((a_0 \oplus a_1) >> (n-t))$，$b_3 = a_0 \oplus ((a_0 \oplus a_1) << t) \oplus (a_1 >> (n-t))$。

若 $a_0 = a_1$，则由定理 3 可知，$b_0, b_1, b_3$ 都不为 0，从而 $b_0, b_1, b_2, b_3$ 中至少有 3 个不为 0。

若 $a_0 \neq a_1$，则由定理 3 可知，$b_0, b_1, b_3$ 中至少有 2 个不为 0，且 $b_2 \neq 0$。从而 $b_0, b_1, b_2, b_3$ 中至少有 3 个不为 0。

3) 设 $a_0, a_1, a_2 \neq 0$ 且 $a_3 = 0$ 时，$b_0, b_1, b_2, b_3$ 中至少有 2 个不为 0。事实上，$a_3 = 0$ 时，有

$$b_0 = a_0 \oplus a_1 \oplus ((a_1 \oplus a_2) << t) \oplus ((a_0 \oplus a_2) >> (n-t))$$
$$b_1 = a_1 \oplus a_2 \oplus ((a_0 \oplus a_2) << t) \oplus ((a_0 \oplus a_1) >> (n-t))$$
$$b_2 = a_2 \oplus ((a_0 \oplus a_1) << t) \oplus ((a_0 \oplus a_1 \oplus a_2) >> (n-t))$$
$$b_3 = a_0 \oplus ((a_0 \oplus a_1 \oplus a_2) << t) \oplus ((a_1 \oplus a_2) >> (n-t))$$

由定理 4 可知，$b_0, b_1, b_2, b_3$ 中至少有 2 个不为 0。

4) 设 $a_0, a_1, a_2, a_3 \neq 0$ 且 $b_0, b_1, b_2, b_3$ 中至少有一个不为 0。事实上，由定理 5 可知，$b_0, b_1, b_2, b_3$ 中至少有一个不为 0。

由 1)～4)及分支数的定理可知，线性变换 $L$ 的分支数为 5，是一个最优线性变换。证毕。

**推论 1**　设 $n$ 是 4 的倍数，$t = \frac{n}{4}$，则 $(F_2^n)^4 \to (F_2^n)^4$ 上基于循环移位–异或型扩散变换 $\boldsymbol{A} \to \boldsymbol{B} : \boldsymbol{B} = \boldsymbol{A} \oplus (\boldsymbol{A} <<< n) \oplus (\boldsymbol{A} <<< (n+3t)) \oplus (\boldsymbol{A} <<< (2n+3t)) \oplus (\boldsymbol{A} <<< (3n+3t))$ 的分支数为 5。

**证明**　由于 $n$ 是 4 的倍数，$t = \frac{n}{4}$，由定理 6 可知 $(F_2^n)^4 \to (F_2^n)^4$ 上基于循环移位–异或型扩散变换 $\boldsymbol{A} \to \boldsymbol{B} : \boldsymbol{B} = \boldsymbol{A} \oplus (\boldsymbol{A} <<< n) \oplus (\boldsymbol{A} <<< (n+t)) \oplus (2n+t)) \oplus (\boldsymbol{A} <<< (3n+t))$ 的分支数为 5。令 $t' = \frac{3n}{4}$，即 $t' = 3t$。与定理 6 的证明过程类似，可得 $\boldsymbol{B} = \boldsymbol{A} \oplus (\boldsymbol{A} <<< n) \oplus (\boldsymbol{A} <<< (n+t')) \oplus (\boldsymbol{A} <<< (2n+t')) \oplus$

$(\boldsymbol{A} <<< (3n+t'))$ 的分支数为 5，是最优线性变换。证毕。

## 3　SPS 结构大规模 S 盒

2 轮 SPS 结构大规模 S 盒如图 1 所示。其基本思想如下：*mn* bit 输入依次进入第一层混淆层、扩散层 *P* 和第二层混淆层，每个混淆层均由 *n* 个 *m* bit 小规模 S 盒并置而成，该小规模 S 盒均选择相同的 *m* bit S 盒，扩散层 *P* 是 *mn* bit 规模的线性置换。*P* 可看作 $(F_2^m)^n \to (F_2^m)^n$ 上基于循环移位–异或型分支数最佳的线性变换。因此，本节主要研究循环移位–异或型最优线性变换。

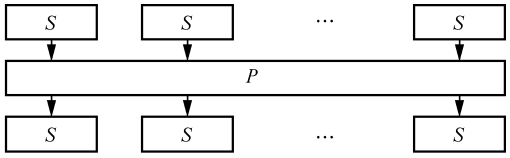


图 1　2 轮 SPS 结构大规模 S 盒

### 3.1　16 bit 最优线性置换

令 *n*=*m*=4，采用循环移位和异或运算组合操作构造线性置换 *P*，使其差分和线性分支数达到最佳 5。对于 SPS 结构中使用的 16 bit 线性置换 *P*，可以统一表示为

$$P(\boldsymbol{x}) = (\boldsymbol{x} <<< t_1) \oplus (\boldsymbol{x} <<< t_2) \oplus (\boldsymbol{x} <<< t_3) \oplus (\boldsymbol{x} <<< t_4) \oplus (\boldsymbol{x} <<< t_5), t_1 = 0$$

其中，$\boldsymbol{x} \in (F_2^4)^4$，循环移位数满足 $0 \leqslant t_i \leqslant n-1$，$i = 1,2,3,4,5$。

根据定理 6，当 *n*=4、*t*=1 时，可得 16 bit 最优线性变换 $P_1(\boldsymbol{x})$ 为

$$P_1(\boldsymbol{x}) = \boldsymbol{x} \oplus (\boldsymbol{x} <<< 4) \oplus (\boldsymbol{x} <<< 5) \oplus (\boldsymbol{x} <<< 9) \oplus (\boldsymbol{x} <<< 13) \tag{10}$$

根据推论 1，当 *n*=4、*t*=3 时，可得 16 bit 最优线性变换 $P_2(\boldsymbol{x})$ 为

$$P_2(\boldsymbol{x}) = \boldsymbol{x} \oplus (\boldsymbol{x} <<< 4) \oplus (\boldsymbol{x} <<< 7) \oplus (\boldsymbol{x} <<< 11) \oplus (\boldsymbol{x} <<< 15) \tag{11}$$

由性质 1 可知，对于线性置换 $P'$，如果其循环移位数满足 $t_i' = (t_i + 4) \bmod 16, i = 1,2,\cdots,5$，则线性置换 *P* 和 $P'$ 的分支数相同.

由性质 2 可知，对于线性置换 $P'$，如果其循环移位数满足 $t_i' = (16 - t_i) \bmod 16, i = 1,2,\cdots,5$，则线性置换 *P* 和 $P'$ 的分支数相同。

考虑到线性置换循环移位等价性质，与置换 $P_1$ 和 $P_2$ 等价的线性置换如表 1 所示。

**表 1　　线性置换 $P_1$ 和 $P_2$ 的等价类**

| 序号 | 线性置换 $P_1$ 的等价类 $\{t_1,t_2,t_3,t_4,t_5\}$ | 线性置换 $P_2$ 的等价类 $\{t_1,t_2,t_3,t_4,t_5\}$ |
|---|---|---|
| 1 | 0,1,5,9,12 | 0,3,7,11,12 |
| 2 | 0,4,5,9,13 | 0,4,7,11,15 |
| 3 | 1,4,8,9,13 | 3,4,8,11,15 |
| 4 | 1,5,8,12,13 | 3,7,8,12,15 |

基于此，小规模 S 盒选用 4 bit 置换，根据图 1 描述的大规模 S 盒模型可以构造一系列具有相同优良密码学性质的 16 bit S 盒。

### 3.2　32 bit/64 bit 最佳线性置换

32 bit/64 bit 最佳线性置换可由 16 bit 最佳线性置换通过一定的规则变换得到，对于 SPS 结构中使用的 32 bit 线性置换 *P*，可以统一表示为

$$P(\boldsymbol{x}) = \boldsymbol{x} \oplus (\boldsymbol{x} <<< t_1) \oplus (\boldsymbol{x} <<< t_2) \oplus (\boldsymbol{x} <<< t_3) \oplus (\boldsymbol{x} <<< t_4)$$

其中，$\boldsymbol{x} \in (F_2^m)^4$，循环移位数满足 $0 \leqslant t_i \leqslant 4m-1$，*i*=1,2,3,4，$m = \dfrac{8}{16}$。

**定理 7**　若两类 16 bit 最佳线性置换如式(10)和式(11)所示，该 16 bit 最佳线性置换对应的循环移位–异或型矩阵为 $\boldsymbol{M}_{4,4}^{I_{16}}$，$\boldsymbol{M}_{4,4}^{I_{16}}$ 是一个 MDS 矩阵，将式(10)和式(11)的循环移位数和模数分别扩大 2 倍，则 32 bit 最佳线性置换的 2 个等价类分别为

$$P_3(\boldsymbol{x}) = \boldsymbol{x} \oplus (\boldsymbol{x} <<< 8) \oplus (\boldsymbol{x} <<< 10) \oplus (\boldsymbol{x} <<< 18) \oplus (\boldsymbol{x} <<< 26) \tag{12}$$

$$P_4(\boldsymbol{x}) = \boldsymbol{x} \oplus (\boldsymbol{x} <<< 8) \oplus (\boldsymbol{x} <<< 14) \oplus (\boldsymbol{x} <<< 22) \oplus (\boldsymbol{x} <<< 30) \tag{13}$$

其中，$\boldsymbol{x} \in (F_2^8)^4$。此时记 32 bit 最佳线性置换对应的循环移位–异或型矩阵为 $\boldsymbol{M}_{4,8}^{I_{32}}$。

**证明**　由于

$$\boldsymbol{M}_{4,4}^{I_{16}} \boldsymbol{x} = \bigoplus_{i \in I} (\boldsymbol{x} <<< i), \boldsymbol{x} \in (F_2^4)^4$$

$$\boldsymbol{M}_{4,4}^{I_{16}} = \mathrm{Circ}(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D})$$

因此

$$2\boldsymbol{M}_{4,4}^{I_{16}} = 2\mathrm{Circ}(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D})$$

$$2\boldsymbol{M}_{4,4}^{I_{16}} \boldsymbol{x}' = \bigoplus_{i \in I} (\boldsymbol{x}' <<< 2i), \boldsymbol{x}' \in (F_2^8)^4$$

令 $\boldsymbol{M}_{4,8}^{I_{32}}\boldsymbol{x}'=2\boldsymbol{M}_{4,4}^{16}\boldsymbol{x}'=\underset{i\in I}{\oplus}(\boldsymbol{x}'<<<2i)$。由引理 1 可知，存在一个常量 $\sigma$=2，使 $\boldsymbol{M}_{4,8}^{I_{32}}=\sigma\boldsymbol{M}_{4,4}^{I_{16}}$。得到 $B_d(\boldsymbol{M}_{4,8}^{I_{32}})=B_d(\boldsymbol{M}_{4,4}^{I_{16}})=5$，因此 $\boldsymbol{M}_{4,8}^{I_{32}}$ 为有限域上的 MDS 矩阵。证毕。

同理，考虑到线性置换循环移位等价性质，与置换 $P_3$ 和 $P_4$ 等价的线性置换如表 2 所示。

**表 2　　线性置换 $P_3$ 和 $P_4$ 的等价类**

| 序号 | 线性置换 $P_3$ 的等价类 $\{t_1,t_2,t_3,t_4,t_5\}$ | 线性置换 $P_4$ 的等价类 $\{t_1,t_2,t_3,t_4,t_5\}$ |
|---|---|---|
| 1 | 0,2,10,18,24 | 0,6,14,22,24 |
| 2 | 0,8,10,18,26 | 0,8,14,22,30 |
| 3 | 2,8,16,18,26 | 6,8,16,22,30 |
| 4 | 2,10,16,24,26 | 6,14,16,24,30 |

根据线性置换循环移位数的等价性质，即 $t_i'=(t_i+8)\bmod 32, i=1,\cdots,5$，可知属于相同等价类的线性置换构造的 32 bit S 盒具有相同的最大差分和线性概率等密码性质。小规模 S 盒选用 8 bit 置换，根据图 1 描述的大规模 S 盒可以构造一系列具有相同优良密码学性质的 32 bit S 盒。

此时记 64 bit 最佳线性置换对应的循环移位–异或型矩阵表示为 $\boldsymbol{M}_{4,8}^{I_{64}}$。

**定理 8**　若两类 16 bit 最佳线性置换如式(10)和式(11)所示，该 16 bit 最佳线性置换对应的循环移位–异或型矩阵为 $\boldsymbol{M}_{4,4}^{I_{16}}$，$\boldsymbol{M}_{4,4}^{I_{16}}$ 是一个 MDS 矩阵。将式(10)和式(11)的循环移位数和模数分别扩大 4 倍，则 64 bit 最佳线性置换的 2 个等价类分别为

$$P_5(\boldsymbol{x})=\boldsymbol{x}\oplus(\boldsymbol{x}<<<16)\oplus(\boldsymbol{x}<<<20)\oplus(\boldsymbol{x}<<<36)\oplus(\boldsymbol{x}<<<52) \tag{14}$$

$$P_6(\boldsymbol{x})=\boldsymbol{x}\oplus(\boldsymbol{x}<<<16)\oplus(\boldsymbol{x}<<<28)\oplus(\boldsymbol{x}<<<44)\oplus(\boldsymbol{x}<<<60) \tag{15}$$

其中，$\boldsymbol{x}\in(F_2^{16})^4$。

**证明**　由于 $\boldsymbol{M}_{4,4}^{I_{16}}\boldsymbol{x}=\underset{i\in I}{\oplus}(\boldsymbol{x}<<<i)$，$\boldsymbol{x}\in(F_2^4)^4$，$\boldsymbol{M}_{4,4}^{I_{16}}=\mathrm{Circ}(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D})$，因此 $4\boldsymbol{M}_{4,4}^{I_{16}}=4\mathrm{Circ}(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D})$，$4\boldsymbol{M}_{4,4}^{I_{16}}\boldsymbol{x}'=\underset{i\in I}{\oplus}(\boldsymbol{x}'<<<4i)$，$\boldsymbol{x}'\in(F_2^{16})^4$

令 $\boldsymbol{M}_{4,16}^{I_{64}}\boldsymbol{x}'=4\boldsymbol{M}_{4,4}^{16}\boldsymbol{x}'=\underset{i\in I}{\oplus}(\boldsymbol{x}'<<<4i)$。由引理 1 可知，存在一个常量 $\sigma$=4，使 $\boldsymbol{M}_{4,16}^{I_{64}}=\sigma\boldsymbol{M}_{4,4}^{16}$。得到 $B_d(\boldsymbol{M}_{4,16}^{I_{64}})=B(\boldsymbol{M}_{4,,4}^{I_{16}})=5$。因此，$\boldsymbol{M}_{4,16}^{I_{64}}$ 为有限域上的 MDS 矩阵。证毕。

同理，考虑到线性置换循环移位等价性质，与置换 $P_5$ 和 $P_6$ 等价的线性置换如表 3 所示。

**表 3　　线性置换 $P_5$ 和 $P_6$ 的等价类**

| 序号 | 线性置换 $P_5$ 的等价类 $\{t_1,t_2,t_3,t_4,t_5\}$ | 线性置换 $P_6$ 的等价类 $\{t_1,t_2,t_3,t_4,t_5\}$ |
|---|---|---|
| 1 | 0,4,20,36,48 | 0,12,28,44,48 |
| 2 | 0,16,20,36,52 | 0,16,28,44,60 |
| 3 | 4,16,32,36,52 | 12,16,32,44,60 |
| 4 | 4,20,32,48,52 | 12,28,32,48,60 |

根据线性置换循环移位数的等价性质，即 $t_i'=(t_i+16)\bmod 64, i=1,\cdots,5$，可知属于相同等价类的线性置换构造的 64 bit S 盒具有相同的最大差分和线性概率等密码性质。小规模 S 盒选用 3.1 节构造的 16 bit 置换，根据图 1 描述的大规模 S 盒可以构造一系列具有相同优良密码学性质的 64 bit S 盒。

## 4　实例分析

### 4.1　16 bit 大规模 S 盒

对于线性变换 $P_2(\boldsymbol{x})=\boldsymbol{x}\oplus(\boldsymbol{x}<<<4)\oplus(\boldsymbol{x}<<<7)\oplus(\boldsymbol{x}<<<11)\oplus(\boldsymbol{x}<<<15)$，采用 2 轮 SPS 结构可以有效生成密码学性质优良且实现代价低廉的 16 bit S 盒。

1) 为便于与现有结果比较，采用与 Piccolo 算法相同的 4 bit S 盒 $S$={10,2,8,6,12,15,7,1,3,11,14,13,0,5,4,9}，使用线性置换 $P_2(\boldsymbol{x})$，按照图 1 所示的 SPS 结构构造 16 bit S 盒 $S_1$，其密码学性质如下：差分均匀度为 Diff($S_1$)=96，最大差分概率为 $\dfrac{96}{65\,536}\approx 2^{-9.41}$，线性度为 Lin($S_1$)=3 200，最大线性概率为 $\left(2\times\dfrac{1\,600}{65\,536}\right)^2\approx 2^{-8.71}$；硬件流水线实现时，$P_2(\boldsymbol{x})$共需要 4 个异或运算和 4 个循环移位，由于比特之间的异或运算大约需要 2 个逻辑门电路，而循环移位靠拉线实现，不占资源，一个 4 bit S 盒大约需要 30 个逻辑门电路，因此共需要 16×4×2+30×8=368 个逻辑门电路；软件实现时，仅需要一次查表。

Piccolo 算法采用了此类 SPS 结构构造的 16 bit S 盒 $S_2$，其中线性层 $P$ 为 4×4 有限域 MDS 矩阵 $\boldsymbol{M}$，其中的乘法运算定义在有限域 $F_2^4$，不可约多项式为

$\boldsymbol{x}^4+\boldsymbol{x}+1$，$\boldsymbol{M}=\begin{bmatrix}2&3&1&1\\1&2&3&1\\1&1&2&3\\3&1&1&2\end{bmatrix}$。该 16 bit S 盒 $S_2$ 的密码学性质如下：差分均匀度为 Diff($S_2$) = 128，最大差分概率为 $\frac{128}{65\,536}=2^{-9}$，线性度为 Lin($S_2$) = 4 096，最大线性概率为 $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$；硬件流水线实现时，MDS 矩阵乘法共需要 6 个异或运算，因此共需要 16×6×2+8×30=432 个逻辑门电路；软件实现时，仅需要一次查表。

NBC 算法采用 Galois 结构的 16 级 NFSR 构造 16 bit S 盒 $S_3$，寄存器每迭代一拍，除常规移位外每拍以非线性方式更新 4 bit，每拍有 8 个异或运算，4 个与运算以及一个与非运算，共迭代 20 拍。该 16 bit S 盒 $S_3$ 的密码学性质如下：差分均匀度为 Diff($S_3$)=22，最大差分概率为 $\frac{22}{65\,536}=2^{-11.541}$，线性度为 Lin($S_3$)=3 144，最大线性概率为 $\left(2\times\frac{1\,572}{65\,536}\right)^2=2^{-10.764}$；硬件流水线实现时，$S_3$ 共需要 20×(8×2+4×1.25+1×1)=440 个逻辑门电路；软件实现时，仅需要一次查表。

与有限域上的 MDS 矩阵乘法运算及 Galois 结构的 16 级非线性移位寄存器运算相比，该类大规模 S 盒的运算代价更加低廉，密码学指标更优，密码学性质对比如表 4 所示。

2) 通过挑选 4 bit 最优 S 盒，结合上述线性置换 $P_2(\boldsymbol{x})$，可以构造密码学性质更优的 16 bit S 盒。考虑到差分和线性性质达到最优 4 bit S 盒分别属于 16 个仿射等价类[32]，通过在这些最优 4 bit S 盒等价类代表元中选择 S 盒进行测试，得到一系列 16 bit S 盒。其构造参数及密码性质如表 5 所示。

由表 5 可见，通过该方式构造的系列 16 bit S 盒的密码性质优良且较为稳定，其最大差分概率集中分布在区间[$2^{-9.83}$, $2^{-8.64}$]，最大线性概率集中分布在区间[$2^{-8.71}$, $2^{-8}$]。与现有的 Piccolo 算法 S 盒相比较，通过本文方法可以得到更优密码学性质的 16 bit S 盒，其 4 bit S 盒 $S$={2,0,1,8,3,11,6,7,4,9,10,15,12,13,14,5}和线性置换 $P_2(\boldsymbol{x})$构造，其密码学性质如下：最大差分概率 $2^{-9.83}$，最大线性概率 $2^{-8.71}$。该 S 盒具有更均衡的抗差分和抗线性攻击能力。

### 4.2　32 bit 大规模 S 盒

对于最优线性变换 $P_3(\boldsymbol{x})$或 $P_4(\boldsymbol{x})$，采用 2 轮 SPS 结构可以有效生成密码学性质优良且实现代价低廉的 32 bit 大规模 S 盒。为了降低资源占用，这里 8 bit S 盒可考虑使用 4 bit 小规模 S 盒（$t_1$、$t_2$ 及 $t_3$）通过 3 轮平衡 Feistel 结构构造得到，如图 2 所示。其中，选用 4 bit $t_i$（$i$=1,2,3）盒的最大差分概率与最大线性概率均为 $2^{-2}$，即 Diff($t_i$)=4，$P\leqslant\frac{4}{16}$，Lin($t_i$)=8，$q\leqslant\left(\frac{8}{16}\right)^2$，使 8 bit 小规模 S 盒的差分概率 $p\leqslant 2^{-4.67}$，线性概率 $q\leqslant 2^{-4}$。基于此类线性置换采用 SPS 结构可以有效构造密码学性质优良且软硬件实现代价低廉的32 bit S盒。其密码学性质如下。

由引理 2 可知，2 轮 SPS 结构构造的 32 bit 大规模置换 S 盒的差分概率上界为 $p^{d-1}$；由引理 3 可知，2 轮 SPS 结构构造的 32 bit 大规模置换 S 盒的线性概率上界为 $q^{d-1}$。

1) 差分均匀度 Diff($S$)=$10^4$，最大差分概率为 $\left(\frac{10}{256}\right)^{d-1}=\frac{10^4}{2^{32}}=0.039\,062\,5^4<2^{-18.68}$。

**表 4　16 bit S 盒 $S_1$、$S_2$ 及 $S_3$ 密码学性质对比**

| S 盒 | 最大差分概率 | 差分均匀度 | 最大线性概率 | 线性度 | ASIC 硬件实现（标准门电路个数）/个 | 软件实现 |
|---|---|---|---|---|---|---|
| $S_1$ SPS:循环移位+异或 | $\frac{96}{65\,536}\approx 2^{-9.41}$ | 96 | $\left(2\times\frac{1\,600}{65\,536}\right)^2\approx 2^{-8.71}$ | 3 200 | 368 | 一次查表 |
| Piccolo 算法 $S_2$ SPS:MDS | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 | 432 | 一次查表 |
| NBC 算法 $S_3$ Galois:16 级 NFSR | $\frac{22}{65\,536}=2^{-11.541}$ | 22 | $\left(2\times\frac{1572}{65\,536}\right)^2=2^{-10.764}$ | 3 144 | 440 | 一次查表 |

**表 5　　2 轮 SPS 结构构造的大规模 S 盒密码学性质**

| 小规模 4 bit S 盒 | 最大差分概率 | 差分均匀度 | 最大线性概率 | 线性度 |
|---|---|---|---|---|
| 4,0,1,15,2,11,6,7,3,9,10,5,12,13,14,8 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{1\,600}{65\,536}\right)^2\approx 2^{-8.71}$ | 3 200 |
| 8,0,1,12,2,5,6,9,4,3,10,11,7,13,14,15 | $\frac{136}{65\,536}\approx 2^{-8.91}$ | 136 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 |
| 8,0,1,12,15,5,6,7,4,3,10,11,9,13,14,2 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{1\,600}{65\,536}\right)^2\approx 2^{-8.71}$ | 3 200 |
| 2,0,1,8,3,13,6,7,4,9,10,5,12,11,14,15 | $\frac{148}{65\,536}\approx 2^{-8.79}$ | 148 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 |
| 2,0,1,8,3,15,6,7,4,9,5,11,12,13,14,10 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{1\,664}{65\,536}\right)^2\approx 2^{-8.59}$ | 3 328 |
| 2,0,1,8,3,11,6,7,4,9,10,15,12,13,14,5 | $\frac{72}{65\,536}\approx 2^{-9.83}$ | 72 | $\left(2\times\frac{1\,600}{65\,536}\right)^2\approx 2^{-8.71}$ | 3 200 |
| 4,8,1,2,3,11,6,7,0,9,10,14,12,13,5,15 | $\frac{164}{65\,536}\approx 2^{-8.64}$ | 164 | $\left(2\times\frac{1\,600}{65\,536}\right)^2\approx 2^{-8.71}$ | 3 200 |
| 8,0,1,9,2,5,13,7,4,6,10,11,12,3,14,15 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{1\,600}{65\,536}\right)^2\approx 2^{-8.71}$ | 3 200 |
| 8,14,1,2,3,5,6,7,4,12,10,11,9,13,0,15 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 |
| 8,14,1,2,3,5,6,7,4,9,15,11,12,13,0,10 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 |
| 8,15,1,2,3,5,12,7,4,9,10,11,6,13,14,0 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 |
| 8,15,1,2,3,5,6,13,4,9,10,11,12,7,14,0 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{1\,792}{65\,536}\right)^2\approx 2^{-8.38}$ | 3 584 |
| 12,0,1,9,3,5,4,7,6,2,10,11,8,13,14,15 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 |
| 12,11,1,2,3,5,4,7,6,9,10,0,8,13,14,15 | $\frac{144}{65\,536}\approx 2^{-8.83}$ | 144 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 |
| 12,9,1,2,3,5,4,7,6,0,10,11,8,13,14,15 | $\frac{132}{65\,536}\approx 2^{-8.95}$ | 132 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 |
| 8,14,1,2,3,5,4,7,6,9,10,0,12,13,11,15 | $\frac{128}{65\,536}=2^{-9}$ | 128 | $\left(2\times\frac{2\,048}{65\,536}\right)^2=2^{-8}$ | 4 096 |

2) 线性度为 $\mathrm{Lin}(S)=2^{24}$，最大线性概率为 $(2^{-4})^{d-1}=(2^{-4})^4=\left(\frac{2^{24}}{2^{32}}\right)^2$。

3) 硬件流水线实现时，$P_3(\boldsymbol{x})$或 $P_4(\boldsymbol{x})$共需要 4 个异或运算和 4 个循环移位，由于比特位之间的异或运算大约需要2个逻辑门电路，而循环移位靠拉线实现，不占资源，如图 2 所示的 8 bit S 盒需要 3 个 4 bit 异或运算和 3 个 4 bit T 盒运算，因此，共需要 32×4×2+8×(3×4×2+3×30)=1 168 个逻辑门电路。

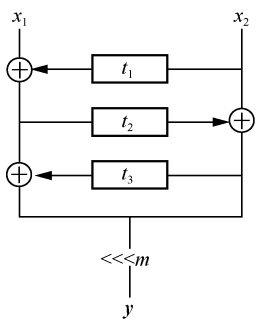


图 2　3 轮平衡 Feistel 结构构造的 8 bit S 盒

SPRING 算法[10]的 32 bit S 盒迭代 32 拍，每拍需要 4 个移位寄存器和 4 个反馈函数运算，移位寄存器共需要 32×6=192 个逻辑门电路，反馈函数需要 4×2×2+6=22 个逻辑门电路，一拍 S 盒共需要 192+22=214 个逻辑门电路。由于一轮 S 盒迭代 32 拍，硬件流水线实现共需要 32×214=6 848 个逻辑门电路。与 SPRING 算法的 32 bit S 盒相比，采用 2 轮 SPS 结构构造的 32 bit S 盒有更优的密码学性质，如表 6 所示。

**表 6 32 bit S 盒密码学性质对比**

| S 盒 | 最大差分概率 | 差分均匀度 | 最大线性概率 | 线性度 | ASIC 硬件实现（标准门电路个数）/个 |
|---|---|---|---|---|---|
| 2 轮 SPS 结构<br>SPS:循环移位+异或 | $\frac{10^4}{2^{32}}$ | $10^4$ | $\left(\frac{2^{24}}{2^{32}}\right)^2$ | $2^{24}$ | 1 168 |
| SPRING 算法 $S_3$<br>Galois:32 bit NFSR | $\frac{40}{2^{32}}$ | 40 | $\left(\frac{119\times 2^{11}}{2^{32}}\right)^2$ | $119\times 2^{11}$ | 6 848 |

### 4.3 64 bit 大规模 S 盒

对于最优线性变换 $P_5(\boldsymbol{x})$或 $P_6(\boldsymbol{x})$，采用 2 轮 SPS 结构可以有效构造密码学性质优良且实现代价低廉的 64 bit 大规模 S 盒。为了降低资源占用，这里的 16 bit S 盒可考虑使用 4 bit 小规模 S 盒通过图 1 的 2 轮 SPS 结构构造得到，如图 3 所示，其中选用的 4 bit $t_i$（$i$=4,5,⋯,11）盒的最大差分概率与最大线性概率均为 $2^{-2}$，即 Diff($t_i$)=4，$P\leqslant\frac{4}{16}$，Lin($t_i$)=8，$q\leqslant\left(\frac{8}{16}\right)^2$，使 16 bit 小规模 S 盒的最大差分概率 $p\leqslant 2^{-9.83}$，线性概率 $q\leqslant 2^{-8.71}$。基于此类线性置换采用 SPS 结构可以有效构造密码学性质优良且软硬件实现代价低廉的 64 bit S 盒。其密码学性质如下。

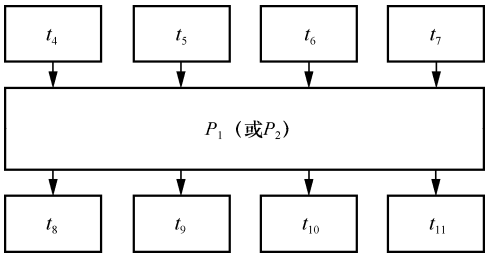


图 3 2 轮 SPS 结构构造的 16 bit S 盒

由引理 2 可知，2 轮 SPS 结构构造的 64 bit 大规模置换 S 盒的差分概率的上界为 $p^{d-1}$；由引理 3 可知，2 轮 SPS 结构构造的 64 bit 大规模置换 S 盒的线性概率的上界为 $q^{d-1}$。

1) 差分均匀度为 Diff($S$)=$72^4$，最大差分概率为 $\left(\frac{72}{2^{16}}\right)^{d-1}=\frac{72^4}{2^{64}}\leqslant(2^{-9.83})^4=2^{-39.32}$。

2) 线性度为 Lin($S$)=3 $200^4$，最大线性概率为

$$\left(\left(\frac{3\,200}{2^{16}}\right)^2\right)^{d-1}=\left(\left(\frac{3\,200}{2^{16}}\right)^{d-1}\right)^2=\left(\frac{3\,200^4}{2^{64}}\right)^2\leqslant(2^{-8.71})^4=2^{-34.84}$$

3) 硬件流水线实现时，$P_3(\boldsymbol{x})$或 $P_4(\boldsymbol{x})$共需要 4 个异或运算和 4 个循环移位，由于比特位之间的异或运算大约需要 2 个逻辑门电路，而循环移位靠拉线实现，不占资源，2 轮 SPS 结构构造的 16 bit S 盒如图 3 所示。16 bit S 盒约需要 368 个逻辑门电路，因此共约需要 64×4×2+8×368=3 456 个逻辑门电路。

Alzette 算法[14]的 64 bit S 盒迭代 4 轮，每轮包含一个 32 bit 整数加法运算、2 个 32 bit 异或运算及 2 个 32 bit 循环右移运算，一个 32 bit 整数加法运算最多需要 200 个逻辑门电路，2 个 32 bit 异或运算约需要 2×2×32=128 个逻辑门电路，循环移位拉线实现不占资源，因此该 64 bit S 盒流水线硬件实现共需要 4×(200+128)=1 312 个逻辑门电路。与 Alzette 算法的 64 bit S 盒相比，采用 2 轮 SPS 结构构造的 64 bit S 盒有更优的密码学性质，如表 7 所示。

**表 7 64 bit S 盒密码学性质对比**

| S 盒 | 最大差分概率 | 差分均匀度 Diff($S$) | 最大线性概率 | 线性度 Lin($S$) | ASIC 硬件实现（标准门电路个数）/个 |
|---|---|---|---|---|---|
| 2 轮 SPS 结构<br>SPS：循环移位+异或 | $\frac{72^4}{2^{64}}$ | $72^4(<2^{32})$ | $\left(\frac{3\,200^4}{2^{64}}\right)^2$ | 3 200($<2^{55.5}$) | 3 456 |
| Alzette 算法 S 盒<br>4 轮 ARX 结构：64 bit | $\frac{2^{32}}{2^{64}}$ | $2^{32}$ | $\left(\frac{2^{55.5}}{2^{64}}\right)^2$ | $2^{55.5}$ | 1 312 |

## 5　结束语

本文基于循环移位与异或运算构造了有限域上分支数最佳的一类线性变换 $P$，给出了该类最优线性变换的一种新的证明方法，建立了 2 轮 SPS 结构的大规模 S 盒模型，通过小规模 S 盒与最优循环移位–异或型线性变换，设计了一系列密码学性质优良的轻量级大规模 S 盒。该设计方案仅使用查表、循环移位、异或三类基本运算，提高了大规模 S 盒的线性度和差分均匀度，与已有大规模 S 盒构造方法相比，本文大规模 S 盒设计方案运算代价更加低廉，其差分、线性等密码学性质更加优良，可应用于对称密码算法非线性置换的设计。

## 参考文献：


[1] LI Y Q, WANG M S. Constructing S-boxes for lightweight cryptography with Feistel structure[C]//International Workshop on Cryptographic Hardware & Embedded Systems. Berlin: Springer, 2014: 127-146.

[2] 龚涛, 陈少真. 基于扩展 Feistel 结构 S 盒的构造分析[J]. 信息工程大学学报, 2017, 18(3): 328-332.
GONG T, CHEN S Z. Analysis of S-boxes with expanded feistel structure[J]. Journal of Information Engineering University, 2017, 18(3): 328-332.

[3] JUNOD P, VAUDENAY S. FOX: a new family of block ciphers[M]. Berlin: Springer, 2004.

[4] CANTEAUT A, DUVAL S, LEURENT G. Construction of lightweight S-boxes using Feistel and MISTY structures[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2015: 373-393.

[5] MATSUI M. New block encryption algorithm MISTY[M]. Berlin: Springer, 1997.

[6] 董新锋, 张文政, 许春香. Feistel 结构的 8 比特轻量化 S 盒[J]. 西安电子科技大学学报, 2021, 48(1): 69-75.
DONG X F, ZHANG W Z, XU C X. 8 bits lightweight S-box with the Feistel structure[J]. Journal of Xidian University, 2021, 48(1): 69-75.

[7] LIU Y, LIU XI L, ZHAO Y M. Security cryptanalysis of NUX for the Internet of things[J]. Security and Communication Networks, 2019: doi.org/10.1155/2019/2062697.

[8] SHIBUTANI K, ISOBE T, HIWATARI H, et al. Piccolo: an ultra-lightweight blockcipher[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2011: 342-357.

[9] 徐洪, 段明, 谭林, 等. NBC 算法[J]. 密码学报, 2019, 6(6): 760-767.
XU H, DUAN M, TAN L, et al. On the NBC algorithm[J]. Journal of Cryptologic Research, 2019, 6(6): 760-767.

[10] 田甜, 戚文峰, 叶晨东, 等. 基于 NFSR 的分组密码算法 SPRING[J]. 密码学报, 2019, 6(6): 815-834.
TIAN T, QI W F, YE C D, et al. SPRING: a family of small hardware-oriented block ciphers based on NFSRs[J]. Journal of Cryptologic Research, 2019, 6(6): 815-834.

[11] National Institute of Standards and Technology. Lightweight crylptography [R]. 2020.

[12] BEIERLE C, BIRYUKOV A, CARDOSO D S L, et al. Lightweight AEAD and hashing using the sparkle permutation family[J]. IACR Transactions on Symmetric Cryptology, 2020(S1): 208-261.

[13] BANIK S, CHAKRABORTI A, IWATA T, et al. GIFT-COFB[J]. Cryptology ePrint Archive, 2020, 738: 1-25.

[14] CHRISTOF B, ALEX B, et al. Alzette: a 64-bit ARX-box (feat. CRAX and TRAX) [C]//Proceedings of the Advances in Cryptology. Berlin: Springer, 2020: 419-448.

[15] NIST. Advanced Encryption Standard(AES)[S]. 2001.

[16] 吴文玲, 张蕾, 郑雅菲, 等. 分组密码 uBlock[J]. 密码学报, 2019, 6(6): 690-703.
WU W L, ZHANG L, ZHENG Y F, et al. The block cipher uBlock[J]. Journal of Cryptologic Research, 2019, 6(6): 690-703.

[17] LIU M C, SIM S M. Lightweight MDS generalized circulant matrices[C]//International Conference on Fast Software Encryption. Berlin: Springer, 2016: 101-120.

[18] 李瑞林, 熊海, 李超. 基于循环移位和异或运算的对合线性变换研究[J]. 国防科技大学学报, 2012, 34(2): 46-50.
LI R L, XIONG H, LI C. Research on involutional linear transformations based on rotation and XOR[J]. Journal of National University of Defense Technology, 2012, 34(2): 46-50.

[19] DONG H C, SANG J L, JONG I L, et al. New block cipher Donut using pairwise perfect decorrelation[C]//Proceedings of the First International Conference on Progress in Cryptology. Berlin: Springer, 2000: 262-270.

[20] CANTEAUT A, DUVAL S, LEURENT G, et al. Saturnin: a suite of lightweight symmetric algorithms for post-quantum security[J]. IACR Transactions on Symmetric Cryptology, 2020(S1): 160-207.

[21] SAJADIEH M, DAKHILALIAN M, MALA H, et al. Recursive diffusion layers for block ciphers and hash functions[C]//International Workshop on Fast Software Encryption. Berlin: Springer, 2012: 385-401.

[22] WU S B, WANG M S, WU W L. Recursive diffusion layers for (lightweight) block ciphers and hash functions[C]//International Conference on Selected Areas in Cryptography. Berlin: Springer, 2013: 355-371.

[23] AUGOT D, FINIASZ M. Direct construction of recursive MDS diffusion layers using shortened BCH codes[C]//International Workshop on

Fast Software Encryption. Berlin: Springer, 2015: 3-17.

[24] LI S, SUN S W, SHI D P, et al. Lightweight iterative MDS matrices: how small can we go?[J]. IACR Transactions on Symmetric Cryptology, 2019(4): 147-170.

[25] LI S, SUN S W, LI C Y, et al. Constructing low-latency involutory MDS matrices with lightweight circuits[J]. IACR Transactions on Symmetric Cryptology, 2019(1): 84-117.

[26] GUO Z, LIU R, WU W, et al. Direct construction of lightweight rotational-XOR MDS diffusion layers[J]. IACR Cryptology ePrint Archive, 2016(1036): 1-16.

[27] GUO Z Y, LIU R Z, GAO S, et al. Direct construction of optimal rotational-XOR diffusion primitives[J]. IACR Transactions on Symmetric Cryptology, 2017(4): 169-187.

[28] 苏俊, 王鑫, 王涛, 等. 循环移位与异或构造扩散层的新证明方法[J]. 密码学报, 2020, 7(6): 763-773.
SU J, WANG X, WANG T, et al. New proof method for cyclic shift and XOR structured diffusion layer[J]. Journal of Cryptologic Research, 2020, 7(6): 763-773.

[29] HONG S, LEE S J, LIM J, et al. Provable security against differential and linear cryptanalysis for the SPN structure[M]. Berlin: Springer, 2001.

[30] BON W K, HWAN S J, JUNG H S. Constructing and cryptanalysis of a 16 × 16 binary matrix as a diffusion layer [C]//International Workshop on Information Security Applications. Berlin: Springer, 2003: 489-503.

[31] 王金波. 基于循环移位构造最优线性变换[C]//中国密码学会 2007 年会论文集. 成都: 西南交通大学出版社, 2007: 306-307.
WANG J B. The optimal permutation in cryptography based on cyclic-shift linear transform[C]//Proceedings of ChinaCrypt 2007. Chengdu: Southwest Jiaotong University Press, 2007: 306-307.

[32] LEANDER G, POSCHMANN A. On the classification of 4 bit S-boxes[M]. Berlin: Springer, 2007.

[作者简介]

**张岚**（1978– ），男，河南南阳人，信息工程大学博士生，主要研究方向为密码学、信息安全等。

**何良生**（1962– ），男，湖南衡阳人，国家密码管理局研究员、信息工程大学博士生导师，主要研究方向为密码学、信息安全等。

**郁滨**（1964– ），男，河南郑州人，信息工程大学教授、博士生导师，主要研究方向为信息安全。