类 MARS 密码结构的线性特性及其优化设计

王念平，洪礼荣
（信息工程大学密码工程学院，河南 郑州 450001）

摘 要：首先，提出了类 MARS 密码结构，给出了该密码结构的若干线性特性，并给出了线性变换的一种优化设计方法。具体地，通过分析一类具有特殊结构的线性逼近的传递规律，证明了无论怎样设计线性变换，$t(1\leqslant t\leqslant 3)$ 轮线性逼近中至少有一条活动轮函数个数为 0 的线性逼近；4 轮线性逼近中至少有一条活动轮函数个数不超过 1 的线性逼近；$t(t>4)$轮线性逼近中至少有一条活动轮函数个数不超过$\lfloor 8t/15\rfloor$的线性逼近。在此基础上，给出了类 MARS 密码结构中线性变换的一种优化设计方法，该优化设计使活动轮函数个数的下界与 MARS 密码结构相比更加接近可能的最大值。

关键词：类 MARS 密码结构；线性逼近；活动轮函数；线性变换
中图分类号：TN918.1
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021068

Linear property and optimal design of MARS-like cryptographic structure

WANG Nianping, HONG Lirong
School of Cryptographic Engineering, Information Engineering University, Zhengzhou 450001, China

Abstract: A MARS-like cryptographic structure was proposed and some linear properties of this cryptographic structure were given. An optimal design method of linear transformation in MARS-like cryptographic structure was also given. Concretely, by analyzing the transfer law of a class of linear approximation with special structure, regardless of the selected linear bijection, the existence of the linear approximation with 0 active round function in the $t(1\leqslant t\leqslant 3)$ round had been demonstrated. Furthermore, there was at least one with no more than 1, $\lfloor 8t/15\rfloor$ active round function among the 4, $t(t>4)$-round of linear approximation, respectively. On this basis, an optimal design method was proposed to make the lower bound of the number of active round function closer to the maximum possible value than the MARS cryptographic structure for the linear transformation in the MARS-like cryptographic structure.

Keywords: MARS-like cryptographic structure, linear approximation, active round function, linear transformation

1 引言

线性密码分析是 Matsui[1]在 1993 年欧洲密码年会上提出的一种针对迭代型分组密码的已知明文攻击方法，其基本思想是利用分组密码算法中明文、密文和密钥之间的不平衡线性逼近来恢复某些密钥比特。对分组密码而言，线性密码分析经过不断的丰富与发展，已成为最有效的密码分析方法之一。因此，评估分组密码抵抗这一攻击的能力是分组密码设计中必须考虑的问题。

在对分组密码抵抗线性密码分析的能力进行评估时，通常的做法是估计多轮线性逼近中活动轮函数（即输出线性逼近非零的轮函数）或活动 S 盒（即输出线性逼近非零的 S 盒）个数的下界，进而给出最大线性逼近概率的上界。如果该上界足够小，就可以认为分组密码具有较强的抵抗线性密码

收稿日期：2020−10−16；**修回日期**：2021−02−22
基金项目：国家自然科学基金资助项目（No.61672031）
Foundation Item: The National Natural Science Foundation of China (No.61672031)

分析的能力。因此，活动轮函数或活动 S 盒的个数是评估分组密码抵抗线性密码分析能力的重要指标。

MARS 密码结构[2-4]（如图 1 所示）是一种典型的密码结构，例如 AES（advanced encryption standard）竞赛的 5 个最终候选算法之一的 MARS[2]就采用了这样的结构。针对 MARS 密码结构，人们进行了深入的研究。文献[3]研究了 MARS 密码结构的随机性。文献[5-7]对 MARS 密码结构或嵌套代替−置换网络（SPN, substitution-permutation network）的 MARS 密码结构抵抗线性密码分析的能力进行了详细的分析。文献[8]利用不可能差分归一化（UID, unified impossible differential）方法找到了广义 MARS 密码结构的 11 轮不可能差分。文献[9]研究了类 MARS 密码结构的不可能差分，证明了 n 分支类 MARS 密码结构存在 $3n-1$ 轮不可能差分，且当 n 是奇数时，任意轮结构均存在不可能差分。文献[10]进一步研究嵌套 SPN 结构的类 MARS 密码结构，将不可能差分的长度扩展至 12 轮，且这个结果与轮函数和扩散层的结构无关。文献[11]针对嵌套 SPN 结构的 MARS 密码结构，利用计算机搜索算法找到了 1~21 轮差分特征中活动 S 盒个数的下界，并指出该算法可直接用于线性密码分析，即通过考虑对偶结构来计算线性逼近中活动 S 盒个数的下界。文献[12]证明了 MARS 密码结构和 SMS4 密码结构[4]之间存在差分−线性对偶性，再结合文献[13]对 SMS4 密码结构的评估结果，给出目前针对 MARS 密码结构的多轮线性逼近中活动轮函数个数下界的最新理论成果。具体地，对于 MARS 密码结构，当轮函数是双射时，$5i+j(i\geqslant 0, 0\leqslant j\leqslant 4)$ 轮线性逼近至少有 $2i+\lfloor j/4\rfloor$ 个活动轮函数，其中 $\lfloor x\rfloor$ 表示不大于 x 的最大整数（下同）。

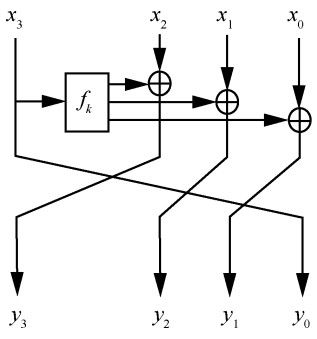


图 1 MARS 密码结构

现在的问题是对于如图 1 所示的 MARS 密码结构，如果将其中的线性变换（即循环左移变换）用 $\{0,1\}^4$ 上的某个线性双射（对应于某个 4 阶 0,1 可逆矩阵）代替，那么活动轮函数个数的下界可能达到的最大值是多少？另外，能否找到一种线性双射，使活动轮函数个数的下界达到或接近可能的最大值？基于这种想法，本文提出了类 MARS 密码结构，如图 2 所示，研究了该密码结构的线性特性，并给出了线性变换的一种优化设计方法。这里所说的类 MARS 密码结构是指每一轮中的线性变换从 $\{0,1\}^4$ 上的线性双射（对应于 4 阶 0,1 可逆矩阵）中选取。在此特别指出，每一轮中的线性变换从 $\{0,1\}^4$ 上的线性双射中选取并不是说 $\{0,1\}^4$ 上的每一个线性双射都是合适的。例如，恒等映射作为每一轮中的线性变换显然就不合适。事实上，在实际的密码设计中，每一轮中的线性变换一般从那些性能较好的、合适的线性双射中选取。

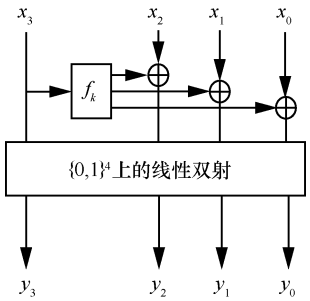


图 2 类 MARS 密码结构

本文的研究结果表明，对于类 MARS 密码结构，每一轮中的线性变换只要从 $\{0,1\}^4$ 上的线性双射中选取，无论怎样设计线性变换，$t(1\leqslant t\leqslant 3)$ 轮线性逼近中都至少有一条线性逼近，其活动轮函数的个数为 0；4 轮线性逼近中至少有一条线性逼近，其活动轮函数的个数≤1；$t(t>4)$ 轮线性逼近中至少有一条线性逼近，其活动轮函数的个数≤$\lfloor 8t/15\rfloor$。这些线性逼近是由类 MARS 密码结构本身决定的，或者说是固有的线性特性。在此基础上，本文给出了线性变换的一种优化设计方法，该优化设计使活动轮函数个数的下界与 MARS 密码结构相比更加接近可能的最大值。

2 预备知识

定义 1[14] 设 $F: Z_2^m \to Z_2^n$ 是多输出布尔函数，$\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_m)\in Z_2^m$，$x=(x_1,x_2,\cdots,x_m)\in Z_2^m$，$\beta=(\beta_1,\beta_2,\cdots,\beta_n)\in Z_2^n$，$F=(F_1,F_2,\cdots,F_n)\in Z_2^n$。记

$\alpha\cdot x=\alpha_1x_1\oplus\alpha_2x_2\oplus\cdots\oplus\alpha_mx_m$ ，　$\beta\cdot F(x)=\beta_1F_1\oplus\beta_2F_2\oplus\cdots\oplus\beta_nF_n$，并记 $\rho=\rho_F(\alpha\to\beta)=W_{(\beta F)}(\alpha)=\frac{1}{2^m}\sum_{x\in Z_2^m}(-1)^{\beta\cdot F(x)\oplus\alpha\cdot x}$，则称 $\alpha\xrightarrow{\rho}\beta$ 为 F 的一个线性逼近（简记为 $\alpha\to\beta$）。其中 $\alpha_i(1\leqslant i\leqslant m)$ 表示 α 的第 i 比特（按照从左到右的顺序计数，x_i 和 β_i 的含义类同），$\alpha\cdot x$ 和 $\beta\cdot F(x)$ 都表示点乘（简记为 αx 和 $\beta F(x)$）。

定义 2[15]　设 $\alpha\to\beta$ 是轮函数的一个线性逼近，若 $\beta\neq0$，则称该轮函数为活动轮函数。

定义 3[16]　迭代分组密码的一条 i 轮线性逼近 $\Lambda=(\beta_0,\beta_1,\cdots,\beta_i)$ 是指输入掩码为 β_0 在 i 轮加密的过程中，中间状态 Y_j 的掩码为 β_j，其中，$1\leqslant j\leqslant i$。

由图 2 可知，1 轮类 MARS 密码结构的输入与输出的关系式可以表示为

$$Q_k(x_3,x_2,x_1,x_0)=(x_3,x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),\ x_0\oplus f_k(x_3))\boldsymbol{N}$$

其中，k 表示轮密钥，$\oplus$ 表示异或运算，f_k 表示轮函数，$\boldsymbol{N}$ 表示 $\{0,1\}^4$ 上的线性双射所对应的 4 阶 0,1 可逆矩阵，并记 $\boldsymbol{N}=(n_{ij})_{0\leqslant i,j\leqslant3},n_{ij}\in\{0,1\}$。这里，$(x_3,x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),x_0\oplus f_k(x_3))\boldsymbol{N}$ 表示 4 个分支 $(x_3,x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),x_0\oplus f_k(x_3))$ 构成的向量与矩阵 $\boldsymbol{N}$ 相乘。例如，当 $(x_3,x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),\ x_0\oplus f_k(x_3))=(11,01,10,00)$ 且 $\boldsymbol{N}=\begin{bmatrix}1&0&0&0\\0&1&1&0\\1&0&1&0\\1&0&0&1\end{bmatrix}$ 时，有

$$(11,01,10,00)\boldsymbol{N}=(11,01,10,00)\begin{bmatrix}1&0&0&0\\0&1&1&0\\1&0&1&0\\1&0&0&1\end{bmatrix}=$$

$$(11\oplus10\oplus00,01,01\oplus10,00)=(01,01,11,00)$$

显然，对于类 MARS 密码结构，线性逼近 $(0,0,0,0)\to(0,0,0,0)$ 的概率恒为 1。此时，称 $(0,0,0,0)\to(0,0,0,0)$ 为平凡线性逼近，否则称其为非平凡线性逼近，以下考虑的都是非平凡线性逼近的情形。

3　类 MARS 密码结构的线性特性分析

首先，给出 3 个引理。

引理 1　设 1 轮类 MARS 密码结构为

$$Q_k(x_3,x_2,x_1,x_0)=(x_3,x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),\ x_0\oplus f_k(x_3))\boldsymbol{N}$$

则 $Q_k(x_3,x_2,x_1,x_0)$ 的具有非零概率的线性逼近都具有 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\to(\alpha_3\oplus\gamma,\alpha_2,\alpha_1,\alpha_0)(\boldsymbol{N}^{\mathrm{T}})^{-1}$ 的形式，且轮函数 f_k 对应的线性逼近为 $\gamma\to\alpha_0\oplus\alpha_1\oplus\alpha_2$。其中，$\alpha_i$ 表示分支 x_i 处的线性逼近，$0\leqslant i\leqslant3$（下同）。

证明　设 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\to(\beta_3,\beta_2,\beta_1,\beta_0)$ 是 $Q_k(x_3,x_2,x_1,x_0)$ 的具有非零概率的线性逼近，且令 $(\beta_3',\beta_2',\beta_1',\beta_0')=(\beta_3,\beta_2,\beta_1,\beta_0)\boldsymbol{N}^{\mathrm{T}}$，则

$$\begin{aligned}&(\alpha_3,\alpha_2,\alpha_1,\alpha_0)(x_3,x_2,x_1,x_0)^{\mathrm{T}}\oplus\\&(\beta_3,\beta_2,\beta_1,\beta_0)Q_k(x_3,x_2,x_1,x_0)^{\mathrm{T}}=\\&(\alpha_3,\alpha_2,\alpha_1,\alpha_0)(x_3,x_2,x_1,x_0)^{\mathrm{T}}\oplus(\beta_3,\beta_2,\beta_1,\beta_0)\cdot\\&((x_3,x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),x_0\oplus f_k(x_3))\boldsymbol{N})^{\mathrm{T}}=\\&(\alpha_3,\alpha_2,\alpha_1,\alpha_0)(x_3,x_2,x_1,x_0)^{\mathrm{T}}\oplus(\beta_3,\beta_2,\beta_1,\beta_0)\boldsymbol{N}^{\mathrm{T}}\cdot\\&(x_3,x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),x_0\oplus f_k(x_3))^{\mathrm{T}}=\\&(\alpha_3,\alpha_2,\alpha_1,\alpha_0)(x_3,x_2,x_1,x_0)^{\mathrm{T}}\oplus(\beta_3',\beta_2',\beta_1',\beta_0')\cdot\\&(x_3,x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),x_0\oplus f_k(x_3))^{\mathrm{T}}=\\&\alpha_0x_0\oplus\alpha_1x_1\oplus\alpha_2x_2\oplus\alpha_3x_3\oplus\beta_3'x_3\oplus\beta_2'(x_2\oplus\\&f_k(x_3))\oplus\beta_1'(x_1\oplus f_k(x_3))\oplus\beta_0'(x_0\oplus f_k(x_3))=\\&(\alpha_0\oplus\beta_0')x_0\oplus(\alpha_1\oplus\beta_1')x_1\oplus(\alpha_2\oplus\beta_2')x_2\oplus\\&(\alpha_3\oplus\beta_3')x_3\oplus(\beta_0'\oplus\beta_1'\oplus\beta_2')f_k(x_3)\end{aligned}\tag{1}$$

其中，上标 T 表示矩阵的转置。若 $\alpha_0\oplus\beta_0'$、$\alpha_1\oplus\beta_1'$、$\alpha_2\oplus\beta_2'$ 不全为零，则 $(\alpha_0\oplus\beta_0')x_0\oplus(\alpha_1\oplus\beta_1')x_1\oplus(\alpha_2\oplus\beta_2')x_2$ 是平衡 Boole 函数，而 $(\alpha_0\oplus\beta_0')x_0\oplus(\alpha_1\oplus\beta_1')x_1\oplus(\alpha_2\oplus\beta_2')x_2$ 与 $(\alpha_3\oplus\beta_3')x_3\oplus(\beta_0'\oplus\beta_1'\oplus\beta_2')f_k(x_3)$ 独立，故式(1)的结果也是平衡 Boole 函数，这与条件“具有非零概率的线性逼近”矛盾，故 $\alpha_0\oplus\beta_0'=\alpha_1\oplus\beta_1'=\alpha_2\oplus\beta_2'=0$，于是 $\alpha_0=\beta_0'$，$\alpha_1=\beta_1'$，$\alpha_2=\beta_2'$，再令 $\alpha_3\oplus\beta_3'=\gamma$，从而 $(\beta_3,\beta_2,\beta_1,\beta_0)=(\beta_3',\beta_2',\beta_1',\beta_0')(\boldsymbol{N}^{\mathrm{T}})^{-1}=(\alpha_3\oplus\gamma,\alpha_2,\alpha_1,\alpha_0)(\boldsymbol{N}^{\mathrm{T}})^{-1}$，进而 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\to(\beta_3,\beta_2,\beta_1,\beta_0)$ 就转化为 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\to(\alpha_3\oplus\gamma,\alpha_2,\alpha_1,\alpha_0)\ (\boldsymbol{N}^{\mathrm{T}})^{-1}$。

此时，式 (1) 的结果可进一步化简为 $\gamma x_3\oplus(\alpha_0\oplus\alpha_1\oplus\alpha_2)f_k(x_3)$，故轮函数 f_k 对应的线性逼近为 $\gamma\to\alpha_0\oplus\alpha_1\oplus\alpha_2$，引理 1 结论成立。证毕。

需要指出的是，以下的证明中考虑的都是具有非零概率的线性逼近。

引理 2　设 1 轮类 MARS 密码结构的输入线性

逼近为 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)$，且轮函数 f_k 对应的线性逼近为 $\alpha_0\oplus\alpha_1\oplus\alpha_2\to\alpha_0\oplus\alpha_1\oplus\alpha_2$，则相应的输出线性逼近为 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{N}'$ 且 $\boldsymbol{N}'$ 是可逆的，其中

$$\boldsymbol{N}'=\begin{bmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{bmatrix}(\boldsymbol{N}^{\mathrm{T}})^{-1}$$

证明 由引理 1 可知，当输入线性逼近为 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)$，且轮函数 f_k 对应的线性逼近为 $\alpha_0\oplus\alpha_1\oplus\alpha_2\to\alpha_0\oplus\alpha_1\oplus\alpha_2$ 时，相应的输出线性逼近为

$$(\alpha_3\oplus\alpha_2\oplus\alpha_1\oplus\alpha_0,\alpha_2,\alpha_1,\alpha_0)(\boldsymbol{N}^{\mathrm{T}})^{-1}=$$
$$(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\begin{bmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{bmatrix}(\boldsymbol{N}^{\mathrm{T}})^{-1}=(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{N}'$$

至于 $\boldsymbol{N}'$ 的可逆性，由 $\boldsymbol{N}$ 的可逆性和线性代数知识即知，引理 2 结论成立。证毕。

引理 3 设 $\boldsymbol{B}$ 是 4 阶 0,1 可逆矩阵，并记

$$\begin{aligned}\boldsymbol{\Omega}=\{&(0,0,0,\xi),(0,0,\xi,0),(0,0,\xi,\xi),(0,\xi,0,0),\\&(0,\xi,0,\xi),(0,\xi,\xi,0),(0,\xi,\xi,\xi),(\xi,0,0,0),\\&(\xi,0,0,\xi),(\xi,0,\xi,0),(\xi,0,\xi,\xi),(\xi,\xi,0,0),\\&(\xi,\xi,0,\xi),(\xi,\xi,\xi,0),(\xi,\xi,\xi,\xi)\}\end{aligned}$$

则当 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)$ 遍历 $\boldsymbol{\Omega}$ 时，$(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{B}$ 也遍历 $\boldsymbol{\Omega}$，其中 $\xi\neq 0$ 表示相应分支处的线性逼近（下同）。

证明 令 $\boldsymbol{B}=(b_{ij})_{0\leqslant i,j\leqslant 3},b_{ij}\in\{0,1\}$。当 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\in\boldsymbol{\Omega}$ 时，有 $\alpha_i\in\{0,\xi\},0\leqslant i\leqslant 3$，从而由 $b_{ij}\in\{0,1\}$ 知 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{B}=\left(\bigoplus_{i=0}^{3}b_{(3-i)0}\alpha_i,\bigoplus_{i=0}^{3}b_{(3-i)1}\alpha_i,\bigoplus_{i=0}^{3}b_{(3-i)2}\alpha_i,\bigoplus_{i=0}^{3}b_{(3-i)3}\alpha_i\right)\in\boldsymbol{\Omega}$，即 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{B}\in\boldsymbol{\Omega}$，故当 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\in\boldsymbol{\Omega}$ 时，$(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\to(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{B}$ 是 $\boldsymbol{\Omega}$ 到 $\boldsymbol{\Omega}$ 的映射。另一方面，对 $\forall(\alpha_3,\alpha_2,\alpha_1,\alpha_0),(\alpha_3',\alpha_2',\alpha_1',\alpha_0')\in\boldsymbol{\Omega}$ 且 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\neq(\alpha_3',\alpha_2',\alpha_1',\alpha_0')$，由 $\boldsymbol{B}$ 的可逆性知 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{B}\neq(\alpha_3',\alpha_2',\alpha_1',\alpha_0')\boldsymbol{B}$，故当 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\in\boldsymbol{\Omega}$ 时，$(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\to(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{B}$ 是 $\boldsymbol{\Omega}$ 到 $\boldsymbol{\Omega}$ 的单射。再由 $\boldsymbol{\Omega}$ 是有限集知，当 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\in\boldsymbol{\Omega}$ 时，$(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\to(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{B}$ 是 $\boldsymbol{\Omega}$ 到 $\boldsymbol{\Omega}$ 的双射。于是，当 $(\alpha_3,\alpha_2,\alpha_1,\alpha_0)$ 遍历 $\boldsymbol{\Omega}$ 时，$(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\boldsymbol{B}$ 也遍历 $\boldsymbol{\Omega}$，引理 3 结论成立。证毕。

定理 1 对于图 2 所示的类 MARS 密码结构，有以下结论成立。

结论 1 $t(1\leqslant t\leqslant 3)$ 轮线性逼近中至少有一条线性逼近，其活动轮函数的个数为 0。

结论 2 4 轮线性逼近中至少有一条线性逼近，其活动轮函数的个数≤1。

证明 由引理 2，考虑如下 15 条 $t(1\leqslant t\leqslant 4)$ 轮线性逼近

$$\begin{aligned}&(0,0,0,\xi)\to(0,0,0,\xi)\boldsymbol{N}'\to(0,0,0,\xi)(\boldsymbol{N}')^2\\&\to\cdots\to(0,0,0,\xi)(\boldsymbol{N}')^t\\&(0,0,\xi,0)\to(0,0,\xi,0)\boldsymbol{N}'\to(0,0,\xi,0)(\boldsymbol{N}')^2\\&\to\cdots\to(0,0,\xi,0)(\boldsymbol{N}')^t\\&(0,0,\xi,\xi)\to(0,0,\xi,\xi)\boldsymbol{N}'\to(0,0,\xi,\xi)(\boldsymbol{N}')^2\\&\to\cdots\to(0,0,\xi,\xi)(\boldsymbol{N}')^t\\&\qquad\qquad\vdots\\&\xi,\xi,\xi,\xi)\to(\xi,\xi,\xi,\xi)\boldsymbol{N}'\to(\xi,\xi,\xi,\xi)(\boldsymbol{N}')^2\\&\to\cdots\to(\xi,\xi,\xi,\xi)(\boldsymbol{N}')^t\end{aligned}\tag{2}$$

其中，每一轮中的轮函数相应的线性逼近为 $0\to 0$ 或 $\xi\to\xi(\xi\neq 0)$，$\boldsymbol{N}'$ 的含义见引理 2，$(\boldsymbol{N}')^j(1\leqslant i\leqslant t)$ 表示 N' 的 i 次幂。设 $\beta_{j,i,k}\in\{0,\xi\}(1\leqslant j\leqslant 15,1\leqslant i\leqslant 4,2\leqslant k\leqslant 4)$ 为第 j 条线性逼近中第 i 轮输入线性逼近的第 k 个分量（例如 $\beta_{1,1,k}(2\leqslant k\leqslant 4)$ 分别为第 1 条线性逼近中第 1 轮输入线性逼近 $(0,0,0,\xi)$ 的第 2~4 个分量 0、0、ξ，依次类推），并记向量 $\left(\bigoplus_{k=2}^{4}\beta_{j,1,k},\bigoplus_{k=2}^{4}\beta_{j,2,k},\bigoplus_{k=2}^{4}\beta_{j,3,k},\cdots,\bigoplus_{k=2}^{4}\beta_{j,t,k}\right)$ 的重量为 W_t（W_t 的值等于该向量中非零元素的个数，因为 $\beta_{j,i,k}\in\{0,\xi\}$，所以也等于该向量中值等于 ξ 的个数），则第 j 条线性逼近中活动轮函数的个数即为 W_t。下面，用反证法进行证明。

先证结论 1。

假设对 $\forall j,1\leqslant j\leqslant 15$，$W_t\geqslant 1$，则由 $\beta_{j,i,k}\in\{0,\xi\}$ 知，$\left(\bigoplus_{k=2}^{4}\beta_{j,1,k},\bigoplus_{k=2}^{4}\beta_{j,2,k},\bigoplus_{k=2}^{4}\beta_{j,3,k},\cdots,\bigoplus_{k=2}^{4}\beta_{j,t,k}\right)$ 最多有 $C_t^1+C_t^2+\cdots C_t^t=2^t-1$ 种不同取值（C_t^i 表示从 t 个不同元素中取 i 个的组合数，下同），而对应于式(2)中的 15 条线性逼近，该向量有 15 种取值（这些取值中可能有重复），又 $1\leqslant t\leqslant 3$ 时 $2^t-1<15$，故由组合论知识知，存在

$p,q,1\leqslant p,q\leqslant 15$，使 $\left(\bigoplus_{k=2}^{4}\beta_{p,1,k},\bigoplus_{k=2}^{4}\beta_{p,2,k},\bigoplus_{k=2}^{4}\beta_{p,3,k},\cdots,\bigoplus_{k=2}^{4}\beta_{p,t,k}\right)=\left(\bigoplus_{k=2}^{4}\beta_{q,1,k},\bigoplus_{k=2}^{4}\beta_{q,2,k},\bigoplus_{k=2}^{4}\beta_{q,3,k},\cdots,\bigoplus_{k=2}^{4}\beta_{q,t,k}\right)$，不妨设 $p=1,q=2$，则 $\left(\bigoplus_{k=2}^{4}\beta_{1,1,k},\bigoplus_{k=2}^{4}\beta_{1,2,k},\bigoplus_{k=2}^{4}\beta_{1,3,k},\cdots,\bigoplus_{k=2}^{4}\beta_{1,t,k}\right)=\left(\bigoplus_{k=2}^{4}\beta_{2,1,k},\bigoplus_{k=2}^{4}\beta_{2,2,k},\bigoplus_{k=2}^{4}\beta_{2,3,k},\cdots,\bigoplus_{k=2}^{4}\beta_{2,t,k}\right)$。于是由式(2)中的第 1 条和第 2 条线性逼近可以“组合”得到如下的 $t(1\leqslant t\leqslant 3)$ 轮线性逼近

$$((0,0,0,\xi)\oplus(0,0,\xi,0))\to((0,0,0,\xi)\oplus(0,0,\xi,0))\boldsymbol{N}'\to((0,0,0,\xi)\oplus(0,0,\xi,0))(\boldsymbol{N}')^2\to\cdots\to((0,0,0,\xi)\oplus(0,0,\xi,0))(\boldsymbol{N}')^t$$

由 $\left(\bigoplus_{k=2}^{4}\beta_{1,1,k},\bigoplus_{k=2}^{4}\beta_{1,2,k},\bigoplus_{k=2}^{4}\beta_{1,3,k},\cdots,\bigoplus_{k=2}^{4}\beta_{1,t,k}\right)=\left(\bigoplus_{k=2}^{4}\beta_{2,1,k},\bigoplus_{k=2}^{4}\beta_{2,2,k},\bigoplus_{k=2}^{4}\beta_{2,3,k},\cdots,\bigoplus_{k=2}^{4}\beta_{2,t,k}\right)$ 知，该线性逼近必具有 $\bigoplus_{k=2}^{4}\left(\beta_{1,i,k}\oplus\beta_{2,i,k}\right)=0,1\leqslant i\leqslant 4$。再由 $(0,0,0,\xi)\oplus(0,0,\xi,0)=(0,0,\xi,\xi)$ 知，该线性逼近就是式(2)中的第 3 条线性逼近。显然，该线性逼近中活动轮函数的个数为 0，这与假设“$\forall j,1\leqslant j\leqslant 15$，$W_t\geqslant 1$”矛盾，故必存在某个 $j,1\leqslant j\leqslant 15$，使 $W_t=0$，结论 1 成立。

再证结论 2。

假设对 $\forall j,1\leqslant j\leqslant 15$，$W_4\geqslant 2$，则由 $\beta_{j,i,k}\in\{0,\xi\}$ 知，$\left(\bigoplus_{k=2}^{4}\beta_{j,1,k},\bigoplus_{k=2}^{4}\beta_{j,2,k},\bigoplus_{k=2}^{4}\beta_{j,3,k},\bigoplus_{k=2}^{4}\beta_{j,4,k}\right)$ 最多有 $C_4^2+C_4^3+C_4^4=11$ 种不同取值。因 $11<15$，故与结论 1 的证明过程类似，可“组合”得到一条满足如下性质的线性逼近：$\bigoplus_{k=2}^{4}\left(\beta_{1,i,k}\oplus\beta_{2,i,k}\right)=0,1\leqslant i\leqslant 4$。该线性逼近就是式(2)中的第 3 条（仍然不妨设 $p=1,q=2$）。显然，该线性逼近中活动轮函数的个数为 0，这与假设“$\forall j,1\leqslant j\leqslant 15$，$W_4\geqslant 2$”矛盾，故必存在某个 $j,1\leqslant j\leqslant 15$，使 $W_4\leqslant 1$，结论 2 成立。证毕。

定理 1 实际上是说，无论每一轮中的线性变换怎样设计，$t(1\leqslant t\leqslant 3)$ 轮线性逼近的活动轮函数个数的下界只能为 0；4 轮线性逼近的活动轮函数个数的下界 $\leqslant 1$。

定理 2　对于图 2 所示的类 MARS 密码结构，$t(t>4)$ 轮线性逼近中至少有一条线性逼近，其活动轮函数的个数 $\leqslant\lfloor 8t/15\rfloor$。

证明　由引理 2，考虑如下 15 条 t 轮线性逼近

$$\begin{aligned}
&(0,0,0,\xi)\xrightarrow{u_1^{(1)}}(0,0,0,\xi)\boldsymbol{N}'\xrightarrow{u_1^{(2)}}(0,0,0,\xi)(\boldsymbol{N}')^2\xrightarrow{u_1^{(3)}}\cdots\xrightarrow{u_1^{(t)}}(0,0,0,\xi)(\boldsymbol{N}')^t\\
&(0,0,\xi,0)\xrightarrow{u_2^{(1)}}(0,0,\xi,0)\boldsymbol{N}'\xrightarrow{u_2^{(2)}}(0,0,\xi,0)(\boldsymbol{N}')^2\xrightarrow{u_2^{(3)}}\cdots\xrightarrow{u_2^{(t)}}(0,0,\xi,0)(\boldsymbol{N}')^t\\
&(0,0,\xi,\xi)\xrightarrow{u_3^{(1)}}(0,0,\xi,\xi)\boldsymbol{N}'\xrightarrow{u_3^{(2)}}(0,0,\xi,\xi)(\boldsymbol{N}')^2\xrightarrow{u_3^{(3)}}\cdots\xrightarrow{u_3^{(t)}}(0,0,\xi,\xi)(\boldsymbol{N}')^t\\
&\qquad\vdots\\
&(\xi,\xi,\xi,\xi)\xrightarrow{u_{15}^{(1)}}(\xi,\xi,\xi,\xi)\boldsymbol{N}'\xrightarrow{u_{15}^{(2)}}(\xi,\xi,\xi,\xi)(\boldsymbol{N}')^2\xrightarrow{u_{15}^{(3)}}\cdots\xrightarrow{u_{15}^{(t)}}(\xi,\xi,\xi,\xi)(\boldsymbol{N}')^t
\end{aligned}\tag{3}$$

其中，每一轮中的轮函数相应的线性逼近同定理 1，$\boldsymbol{N}'$ 的含义见引理 2，$(\boldsymbol{N}')^i(1\leqslant i\leqslant t)$ 表示 $\boldsymbol{N}'$ 的 i 次幂，$u_j^{(i)}(1\leqslant j\leqslant 15,1\leqslant i\leqslant t)$ 表示第 j 条线性逼近中第 i 轮的活动轮函数的个数（$u_j^{(i)}=0$ 表示第 j 条线性逼近中第 i 轮的轮函数是不活动的，即轮函数的线性逼近为 $0\to 0$；$u_j^{(i)}=1$ 表示第 j 条线性逼近中第 i 轮的轮函数是活动的，即轮函数的线性逼近为 $\xi\to\xi(\xi\neq 0)$）。显然，式(3)中的 15 条线性逼近的输入线性逼近遍历 $\boldsymbol{\Omega}$（$\boldsymbol{\Omega}$ 的含义同引理 3），故这 15 条线性逼近中第 1 轮的活动轮函数个数之和为 8，即 $u_1^{(1)}+u_2^{(1)}+\cdots+u_{15}^{(1)}=8$。由引理 2 知 $\boldsymbol{N}'(1\leqslant i\leqslant t)$ 是可逆的，从而再由引理 3 知，对 $\forall v,1\leqslant v\leqslant t$，向量 $((0,0,0,\xi)(\boldsymbol{N}')^v,(0,0,\xi,0)(\boldsymbol{N}')^v,\cdots,(\xi,\xi,\xi,\xi)(\boldsymbol{N}')^v)$ 都遍历 $\boldsymbol{\Omega}$，故第 v 轮的活动轮函数个数之和也为 8，即 $u_1^{(v)}+u_2^{(v)}+\cdots+u_{15}^{(v)}=8$。因此，这 15 条 t 轮线性逼近的活动轮函数个数总和为 $8t$，从而至少有 1 条线性逼近的活动轮函数个数 $\leqslant\lfloor 8t/15\rfloor$，定理 2 结论成立。证毕。

定理 2 实际上是说，无论每一轮中的线性变换怎样设计，$t(t>4)$ 轮线性逼近的活动轮函数个数的下界 $\leqslant\lfloor 8t/15\rfloor$。

为方便起见，将定理 1 和定理 2 合写成定理 3。

定理 3　对于图 2 所示的类 MARS 密码结构，$t(t\geqslant 1)$ 轮线性逼近中至少有一条线性逼近，其活动轮函数的个数 $\leqslant L(t)$。其中

$$L(t)=\begin{cases}0, & t=1,2,3\\ 1, & t=4\\ \lfloor 8t/15\rfloor, & t>4\end{cases}$$

由定理 3 知，无论每一轮中的线性变换怎样设计，$t(t>4)$ 轮线性逼近的活动轮函数个数的下界都小于或等于 $L(t)$。

4 线性变换的一种优化设计

本节给出类MARS密码结构中线性变换的一种优化设计方法，该优化设计使活动轮函数个数的下界与MARS密码结构相比更加接近可能的最大值 $L(t)$。

图 3 是一类特殊的类 MARS 密码结构，其中虚线方框部分表示线性变换。由图 3 可知，其 1 轮输入与输出的关系式可以表示为

$$Q_k(x_3,x_2,x_1,x_0)=$$
$$(x_3,x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),x_0\oplus f_k(x_3))\boldsymbol{N}=$$
$$(x_0\oplus x_1\oplus x_2\oplus f_k(x_3),x_1\oplus f_k(x_3),$$
$$x_0\oplus f_k(x_3),x_1\oplus x_2\oplus x_3)$$

其中，k 表示轮密钥，$\oplus$ 表示异或运算，f_k 表示轮函数，$\boldsymbol{N}$ 表示线性变换（即图 3 中虚线方框部分）所对应的 4 阶 0,1 可逆矩阵，$\boldsymbol{N}=\begin{bmatrix}0&0&0&1\\1&0&0&1\\1&1&0&1\\1&0&1&0\end{bmatrix}$。

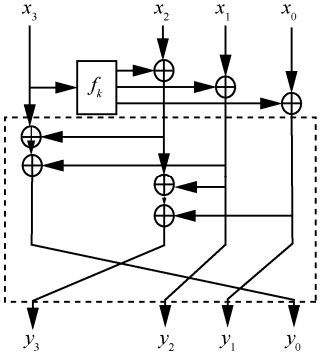


图 3 一类特殊的类 MARS 密码结构

为了直观起见，针对 1~32 轮的情形，将 MARS 密码结构（如图 1 所示）、一类特殊的类 MARS 密码结构（如图 3 所示）的活动轮函数个数的下界与定理 3 中 $L(t)$ 的值进行比较。其中，MARS 密码结构的下界是指图 1 所示的MARS密码结构的活动轮函数个数的下界，该结果由文献[12-13]可得。特殊的类MARS密码结构的下界是指图3的一类特殊的类 MARS 密码结构的活动轮函数个数的下界，该结果可利用与文献[13]类似的推导方法得出，在此不再赘述。

2 种密码结构的活动轮函数个数的下界与 $L(t)$ 的比较如表 1 所示。由表 1 可以看出，当线性逼近的轮数较大时，MARS 密码结构的活动轮函数个数的下界与 $L(t)$ 相比有较大的差距。例如，当线性逼近的轮数≥21时，二者的差值≥3；当线性逼近的轮数≥27时，二者的差值≥4；当线性逼近的轮数为 32 时，二者的差值为 5。但这类特殊的类 MARS 密码结构的活动轮函数个数的下界与 $L(t)$ 更加接近。当线性逼近的轮数为 6、17、19、20、21、23、25、30、31 和 32 时，二者的差值为 2；当线性逼近的轮数为 5、7、8、9、10、11、12、15、16、18、22、24、26、27 和 29 时，二者的差值为 1；其他情形下二者的差值为 0。

以上分析结果表明，从抵抗线性密码分析的角度来讲，这类特殊的类 MARS 密码结构中的线性变换设计得较好。从应用层面来讲，当轮数≥12 时，这类特殊的类 MARS 密码结构的活动轮函数个数的下界比 MARS 密码结构的活动轮函数个数的下界要大，这意味着与 MARS 密码结构相比，采用这类特殊的类 MARS 密码结构的密码算法可以在更少轮数内达到足够的安全强度。从实现效率来讲，这类特殊的类 MARS 密码结构仅增加了少许异或运算，对于算法的实现效率影响不大。

实际上，图 3 中的线性变换（即虚线方框部分）仅仅是一种优化设计方法。除此之外，还有其他的优化设计方法，使在相同的轮数下，活动轮函数个数的下界与 MARS 密码结构相比更接近于 $L(t)$（$L(t)$ 的含义见定理 3）。例如，将图 3 中的线性变换用它的逆变换代替，也可以得到相同的活动轮函数个数的下界。从道理上讲，通过分析全部可能的线性变换，就可以找到类 MARS 密码结构中线性变换的最优化设计，但由于异或运算“⊕”的影响，使搜索到的活动轮函数个数的下界比实际的下界可能要小，因此不能确定图 3 中的线性变换是否最优。如何寻找类 MARS 密码结构中线性变换的最优化设计，还需要进一步的探讨。另外，本文的研究结果表明，无论类 MARS 密码结构中的线性变换怎样设计，多轮线性逼近中活动轮函数个数的下界都不可能超过某个值，这些特性是由类 MARS 密码结构本身决定的，它揭示了类 MARS 密码结构固有的线性特性，这种研究方法对其他分组密码结构的研

表 1　　2 种密码结构的活动轮函数个数的下界与 $L(t)$的比较

线性逼近的轮数	MARS 密码结构的下界	特殊的类 MARS 密码结构的下界	$L(t)$的值	线性逼近的轮数	MARS 密码结构的下界	特殊的类 MARS 密码结构的下界	$L(t)$的值
1	0	0	0	17	6	7	9
2	0	0	0	18	6	8	9
3	0	0	0	19	7	8	10
4	1	1	1	20	8	8	10
5	2	1	2	21	8	9	11
6	2	1	3	22	8	10	11
7	2	2	3	23	8	10	12
8	2	3	4	24	9	11	12
9	3	3	4	25	10	11	13
10	4	4	5	26	10	12	13
11	4	4	5	27	10	13	14
12	4	5	6	28	10	14	14
13	4	6	6	29	11	14	15
14	5	7	7	30	12	14	16
15	6	7	8	31	12	14	16
16	6	7	8	32	12	15	17

究也具有一定的借鉴意义。例如，用本文的研究方法可以证明，对类 SMS4 密码结构（即将 SMS4 密码结构中的线性变换用 $\{0,1\}^4$ 上的线性双射代替），也有与定理 1~定理 3 类似的结论成立。

5　结束语

本文提出了类 MARS 密码结构，通过分析一类具有特殊结构的线性逼近的传递规律，给出了该密码结构的若干线性特性。具体地，不论每一轮的线性变换怎样从 $\{0,1\}^4$ 上的线性双射中选取，$t(1 \leqslant t \leqslant 3)$ 轮线性逼近中至少有一条线性逼近，其活动轮函数的个数为 0；4 轮线性逼近中至少有一条线性逼近，其活动轮函数的个数不超过 1；$t(t > 4)$ 轮线性逼近中至少有一条线性逼近，其活动轮函数的个数不超过$\lfloor 8t/15 \rfloor$。在此基础上，给出了类MARS密码结构中线性变换的一种优化设计方法，该优化设计使活动轮函数个数的下界与 MARS 密码结构相比更加接近可能的最大值 $L(t)$（$L(t)$ 的含义见定理 3），从抵抗线性密码分析的角度来讲，该线性变换设计得较好。

参考文献：

[1] MATSUI M. Linear cryptanalysis method for DES cipher[C]//Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1993: 386-397.

[2] BURWICK C, COPPERSMITH D, AVIGNOND E, et al. MARS: a candidate cipher for AES[R]. IBM Corporation, (1999-09-22)[2020-10-16].

[3] MORIAI S, VAUDENAY S. On the pseudorandomness of top-level schemes of block ciphers[C]// International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2000: 289-302.

[4] 吴文玲, 冯登国, 张文涛. 分组密码的设计与分析(第 2 版)[M]. 北京: 清华大学出版社, 2009.
WU W L, FENG D G, ZHANG W T. Design and analysis of block cipher (the second edition) [M]. Beijing: Tsinghua University Press, 2009.

[5] JUAN M, JOHN A, JULIO C. Non-linear cryptanalysis revisited: heuristic search for approximations to S-boxes [C]// IMA International Conference on Cryptography and Coding. Berlin: Springer, 2007: 99-117.

[6] CASTRO C J H, VILLALBA L J G, CASTRO J C H, et al. On MARS's s-boxes strength against linear cryptanalysis[C]// Internation-

al Conference on Computational Science and Its Applications. Berlin: Springer, 2003: 79-83.

[7] ROBSHAW M, YIN Y. Potential flaws in the conjectured resistance of MARS to linear cryptanalysis (extended abstract) [J]. Radiology, 2000, 276(3): 928-9.

[8] LUO Y Y, LAI X J, WU Z M, et al. A unified method for finding impossible differentials of block cipher structures[J]. Information Sciences, 2014, 263: 211-220.

[9] XUE W J, LAI X J. Impossible differential cryptanalysis of MARS-like structures[J]. IET Information Security, 2015, 9(4): 219-222.

[10] CHENG L, LI C. Revisiting impossible differentials of MARS-like structures[J]. IET Information Security, 2017, 11(5): 273-276.

[11] WU S B, WANG M S. Security evaluation against differential cryptanalysis for block cipher structures[EB]. IACR Cryptology ePrint Archive, 2011.

[12] 崔霆. 不可能差分区分器的构造方法研究[D]. 郑州:信息工程大学, 2013.
CUI T. On constructing impossible differential distinguishers[D]. Zhengzhou: Information Engineering University, 2013.

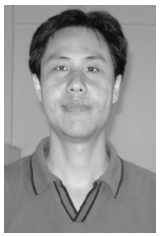
[13] 王念平, 殷勍. SMS4 型密码结构抵抗差分和线性密码分析能力评估[J]. 密码学报, 2015, 2(2): 189-196.
WANG N P, YIN Q. Security evaluation for SMS4-typed ciphers structure against differential and linear cryptanalysis[J]. Journal of Cryptologic Research, 2015, 2(2): 189-196.

[14] 金晨辉, 郑浩然, 张少武, 等. 密码学[M]. 北京:高等教育出版社, 2009.
JIN C H, ZHENG H R, ZHANG S W, et al. Cryptography[M]. Beijing: High Education Press, 2009.

[15] SCHNEIER B, KELSEY J. Unbalanced Feistel networks and block cipher design[C]//International Workshop on Fast Software Encryption. Berlin: Springer, 1996: 121-144.

[16] 李超, 孙兵, 李瑞林. 分组密码的攻击方法与实例分析[M]. 北京: 科学出版社, 2010.
LI C, SUN B, LI R L. The attack method and analysis example of the block cipher[M]. Beijing: Science Press, 2010.

[作者简介]



王念平（1973− ），男，河南洛宁人，博士，信息工程大学教授、博士生导师，主要研究方向为密码学、信息安全等。

洪礼荣（1995− ），男，福建南安人，信息工程大学硕士生，主要研究方向为分组密码的设计与分析等。