Advances in Applied Mathematics 应用数学进展, 2018, 7(4), 429-445
Published Online April 2018 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2018.74054

Hans汉斯

The Construction of Lightweight MDS Matrix

Min Zhou[1], Zhi Gu[2]

[1]Institute of Applied Mathematics in Xihua University, Chengdu Sichuan
[2]Southwest Jiaotong University School of Mathematics, Chengdu Sichuan
Email: 1027164433@qq.com

Received: Apr. 11th, 2018; accepted: Apr. 21st, 2018; published: Apr. 28th, 2018

Abstract

MDS Matrix has important applications in cryptography and it can be used to construct block ciphers. The number of XOR of a MDS Matrix is an important index to measure the validity of cipher algorithm. In this paper, we study the properties of MDS matrix and consider the ideas of cycle, block matrix and so on. The MDS matrix is constructed for several special properties, including cyclic MDS matrix, Hadamard MDS matrix and iterative MDS matrix etc. When the number $m = 4, 8$, we use the program to search the MDS matrix that satisfies the condition. The number of MDS matrix with the minimum number of XOR and examples are given and we get many MDS matrices with the minimum number of XOR; when $m = 4$, we have given the circulating MDS Matrix with the number of XOR with 12, when $m = 8$ we have given the best MDS Matrix with the number of XOR with 10.

Keywords

MDS Matrix, Linear Diffusion Layer, Cyclic Matrix, Hadamard Matrix, Number of XOR

轻量级MDS矩阵的构造

周　敏[1]，顾　执[2]

[1]西华大学数学研究所，四川 成都
[2]西南交通大学数学学院，四川 成都
Email: 1027164433@qq.com

收稿日期：2018年4月11日；录用日期：2018年4月21日；发布日期：2018年4月28日

摘　要

MDS矩阵在密码学中有重要的应用，可以用来构造分组密码。MDS矩阵的异或数是衡量密码算法的有效

文章引用: 周敏, 顾执. 轻量级 MDS 矩阵的构造[J]. 应用数学进展, 2018, 7(4): 429-445.
DOI: 10.12677/aam.2018.74054

性的一个重要指标。本文研究MDS矩阵的性质，考虑循环、矩阵分块和迭代等思想，分别针对几类特殊性质的MDS矩阵构造，包括循环MDS矩阵、Hadar MDS矩阵和迭代MDS矩阵等。在$m = 4, 8$情况下，使用程序来搜索满足条件的MDS矩阵，给出了具有最小异或数的MDS矩阵的数目和例子，得到$m = 4, 8$情况下许多具有已知最小异或数的MDS矩阵，得到了$m = 4$时具有异或数12的循环MDS矩阵，也构造了$m = 8$时具有异或数10的最佳MDS矩阵。

关键词

MDS矩阵，线性扩散层，循环矩阵，Hadamard矩阵，异或数

1. 绪论

1.1. 引言

混乱原则和扩散原则是保证分组密码安全性的重要原则，线性扩散层是分组对称密码算法的重要组成部分，其扩散特性是通过特定的内部结构来实现的。扩散结构的设计十分重要，直接关系到分组密码的安全性能和实现性能[1]。在轻量级加密过程中，通过有限的资源环境保证信息安全，线性扩散层发挥着重要作用。

分支数是分组密码设计中的一个重要组成成分，可以根据分支数的大小从理论上给出差分和线性攻击的抵抗界限。线性扩散层是一个线性变换，可以通过一个 n 阶矩阵表示，若这个 n 阶矩阵的最大分支数是 n + 1，则这个扩散层就称为完美扩散层。MDS 矩阵的分支数达到最大，在分组密码的扩散结构中得到广泛应用，比如 Advanced Encryption Standard (AES) [2]、Shark [3]以及 Twofish [4]和 Khazad [5]分组密码算法等。此外，为了保证解密结构和加密结构的一致性，通常采用对合 MDS 矩阵，因此，如何构造良好性质的对合 MDS 矩阵成为了研究的目标。

构造 MDS 矩阵的方法通常利用有限域及 MDS 码。为提高运算效率，通常考虑有限域上具有较少非零元素的矩阵。循环矩阵以及 Hadamard 矩阵是主要选取的对象，AES 扩散层就是使用此类矩阵。为了适用于轻量密码算法，目前主要使用递归扩散层构造最优扩散层，具体是首先构造一个简单的矩阵，然后该矩阵复合若干次(通常大于等于矩阵的阶数)，得到 MDS 矩阵。在轻量级的 Hash 函数设计中，比如 PHOTON，以及分组密码 LED [6]，均是通过此类 MDS 矩阵构造。利用上述想法并用具有较少异或操作的线性变换替换有限域上的乘法，实现效率得以提高。如何构造轻量级 MDS 矩阵，既能减少矩阵乘法运算中出现的困难又能避免迭代构造出现的问题，是进一步需要研究的问题。

本文考虑 m = 4, 8 时具有小异或数的 MDS 矩阵，首先给出了 MDS 矩阵异或数的性质，然后使用直接搜索满足性质的特殊循环 MDS 矩阵，并分析 MDS 矩阵的异或数最小值和数目，为了改进 MDS 矩阵的构造方法和效率，使用循环、分块和迭代等思想，来考虑特殊 MDS 矩阵，并分析这些 MDS 矩阵的异或数最小值和数目。

本文的主要结构是：第二节给出了一些基本概念和 MDS 矩阵性质；第三节使用循环、分块和迭代等思想，给出几种特殊类型 MDS 矩阵的构造，并分析这些 MDS 矩阵的最小异或数和数目。

1.2. 预备知识

记 F_{2^m} 为一个有 2^m 个元素的有限域，当 $m=1$ 时，值为 0 或 1，F_{2^m} 可以看成 F_2 上的 m 维线性空间，记 F_2^m 为 F_2 上的 m 维线性空间。一个矩阵成为二元矩阵，若矩阵的每个元素都在有限域 F_2 中，即每个元素都是 0 或 1。

一个 $F_2^m \to F_2^m$ 映射 L 被称为是线性的，若 $L(x+y)=L(x)+L(y)$，其中 $x,y \in F_2^m$。确定 F_2^m 上的一个基，F_2^m 上的线性映射可以用 $m\times m$ 的二元矩阵 L 表示，即 $L(x)=Lx$，其中 $x=(x_1,\cdots,x_m)$ 为一个列向量。

记 $GL(m,F_2)$ 为所有的 $m\times m$ 的非奇异二元矩阵的集合，其中 $m=4,8$。取一个二元矩阵

$$L=\begin{pmatrix} L_{1,1} & L_{1,2} & L_{1,3} & L_{1,4} \\ L_{2,1} & L_{2,2} & L_{2,3} & L_{2,4} \\ L_{3,1} & L_{3,2} & L_{3,3} & L_{3,4} \\ L_{4,1} & L_{4,2} & L_{4,3} & L_{4,4} \end{pmatrix}$$

其中 L_{ij} 为 $GL(m,F_2)$ 中一个二元矩阵。定义 L 的一个 t 阶子方阵为 $L(J,K)=\left(L_{j_l,k_p}\right),1\le l\le p\le t$，其中 $J=[j_1,\cdots,j_t]$，$K=[k_1,\cdots,k_t]$ 是两个长度为 t 的序列，并且 $1\le j_1,\cdots,j_t\le 4$，$1\le k_1,\cdots,k_t\le 4$。二元矩阵 L 称为 MDS 矩阵，若 L 的任意阶数为 t 的子方阵都是满秩矩阵。

对任意的二元矩阵 L，记 L 的异或数为 $\#L$，其中 $\#L=\sum_{i=1}^{m}\left(\omega(L[i])-1\right)$，$m$ 为 L 的阶数，$w(L[i])$ 为 L 的第 i 行中 1 的个数。对任意的 $L\in GL(m,F_2)$，通过提取 L 中每一行不为零元素的位置而将 L 的简化形式给出，例如矩阵[[1,3], 2, 3, [1,4]]表示如下矩阵

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

线性扩散层是一个线性变换，每一个线性变换都可以用一个 m 阶矩阵表示。所以每一个线性扩散层都可以有一个 m 阶矩阵表示，众所周知，m 阶矩阵的最大分支数是 $m+1$。具有最大分支数的线性扩散层是一个完美扩散层或者是一个 MDS 矩阵。

一个矩阵被称为循环矩阵，若这个矩阵每一行的最后一个分块被旋转到下一行的最左边。四阶循环矩阵如下

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

其中 $A,B,C,D\in GL(m,F_2)$

一个 $2^k\times 2^k$ 的矩阵被称为 Hadamard 矩阵，若它具有如下形式

$$\begin{pmatrix} H_1 & H_2 \\ H_2 & H_1 \end{pmatrix},$$

其中 H_1,H_2 是两个 $2^{k-1}\times 2^{k-1}$ 的 Hadamard 矩阵。四阶 Hadamard 矩阵如下

$$Had(A,B,C,D)=\begin{pmatrix} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{pmatrix}$$

其中 $A,B,C,D\in GL(m,F_2)$。

文献[7]给出了循环 MDS 矩阵和 Hadamard MDS 矩阵的一个下界，提出一种利用非对合矩阵，建构出异或数较小的 MDS 矩阵，主要的思想是对构造的非对合 MDS 矩阵，通过不同矩阵的性质的研究，借助搜索，得到最终异或数最小的 MDS 矩阵。

2. 构造轻量级 MDS 矩阵

本节主要使用循环、分块和迭代等思想，在 $m=4,8$ 情况下，考虑特殊二元 MDS 矩阵的构造，分别考虑循环 MDS 矩阵、Hadmard MDS 矩阵、最佳 MDS 矩阵和迭代 MDS 矩阵的构造，分析这些矩阵的性质，使用程序搜索具有最小异或数的 MDS 矩阵，并给出了矩阵对应的最小异或数以及这些矩阵的数目，得到了 $m=4$ 时具有异或数 12 的循环 MDS 矩阵(2.1 节)，也构造了 $m=8$ 时具有异或数 10 的最佳 MDS 矩阵(2.4 节)。

2.1. 轻量级循环 MDS 矩阵的构造

对于循环型矩阵

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

若 $L=Circ(A,B,C,D)$ 是 MDS 矩阵，则 A,B,C,D 都必须是可逆矩阵。4 阶可逆矩阵有 20,160 个，而 8 阶可逆矩阵超过了 2^{62} 个。需要构造轻量级 MDS 矩阵，直观看应该包含异或数为 0 的矩阵(置换矩阵)，特别地，我们可将 A,B,C,D 中某些矩阵取为单位阵。因此，首先考虑如下矩阵：

$$L=Circ(I\quad I\quad A\quad B)$$

其中 I 为单位矩阵。首先给出如下基本引理(证明由高等代数基本知识可得证)。

引理 1：假设 $A,B,C\in GL(m,F_2)$ 均是二元域上的 m 阶满秩矩阵，则有下述结论：

1) $\begin{pmatrix} I & A \\ B & C \end{pmatrix}$ 是满秩矩阵当且仅当 $(BA+C)$ 为满秩矩阵。

2) $\begin{pmatrix} A & I \\ B & C \end{pmatrix}$ 是满秩矩阵当且仅当 $(CA+B)$ 为满秩矩阵。

3) $\begin{pmatrix} A & B \\ I & C \end{pmatrix}$ 是满秩矩阵当且仅当 $(AC+B)$ 为满秩矩阵。

4) $\begin{pmatrix} A & B \\ C & I \end{pmatrix}$ 是满秩矩阵当且仅当 $(BC+A)$ 为满秩矩阵。

对于 $L=Circ(I\quad I\quad A\quad B)$ 型矩阵，若 L 为 MDS 矩阵，则必定有以下几个矩阵均为满秩矩阵：

$$A+I,B+I,AB+I,A^2+B,A+B^2,A+B$$

下面针对 $m=4$ 和 $m=8$，分别讨论 MDS 矩阵。

2.1.1. 4 阶矩阵环上的循环型 MDS 矩阵

考虑在 $GL(4,F_2)$ 上的所有满秩矩阵，令集合

$$mzjz=\{A\mid A\in GL(4,F_2)\text{且}A\text{为满秩矩阵}\}$$

为了满足 MDS 矩阵的相关条件，记集合

$$mzjz1=\{B\mid A\in mzjz\text{且}B=A+I\in mzjz\}$$

记满足上述条件的有序矩阵对 (A,B)，其中 $(A,B)\in mzjz1\times mzjz1$

令 $S_{A,B}=\{(A,B)\mid A+I,B+I,AB+I,A^2+B,A+B^2,A+B\in mzjz\}$

最后依照 MDS 矩阵的定义，依次验证 $L=Circ(I\quad I\quad A\quad B)$，其中 $A,B\in S_{A,B}$

使用程序 4 总共搜索到 156,387 个这种形式的 MDS 矩阵，其中异或总数最低的 MDS 矩阵共有 48 个，其异或数为 12。并且，经过验证，A、B 满足关系：

$A=B^{-2}$ 或 $B=A^{-2}$。

例 1：$A=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&1\\1&1&0&0\end{pmatrix},B=\begin{pmatrix}1&0&1&0\\1&0&0&0\\0&0&0&1\\0&1&0&0\end{pmatrix},L=Circ(I\quad I\quad A\quad B)$

例 2：$A=\begin{pmatrix}0&0&0&1\\0&0&1&0\\1&0&0&0\\0&1&0&1\end{pmatrix},B=\begin{pmatrix}0&1&0&0\\1&0&1&0\\1&0&0&1\\0&0&1&0\end{pmatrix},L=Circ(I\quad I\quad A\quad B)$

2.1.2. 8 阶矩阵环上的循环型 MDS 矩阵

当 $m=8$ 时，若依照 $m=4$ 的程序搜索方法，面临搜索数据量极大的问题。为缩小搜索范围，考虑特殊情形下的这类 MDS 矩阵，分别在两种具体情形下讨论。

1) 基于低异或数子类搜索：

利用分块构造矩阵的思想，具体考虑这样形式的集合：

$$mzjz2=\left\{A\middle|A=\begin{pmatrix}A_{11}&A_{12}\\A_{21}&A_{22}\end{pmatrix},\text{其中}A_{ij}\in GL(4,F_2)\text{且}rand(A)=8\right\}$$

考虑 $mzjz2$ 中的矩阵 A 的限定条件：

a) 取 $\begin{cases}A_{11}=A_{22}\in X(\text{异或数小于1的所有二元矩阵,保存于元胞数组小于1})\\A_{21}=A_{12}=CI(\text{次对角线元素为1,其余元素为0})\end{cases}$，

即 $A=\begin{pmatrix}X&CI\\CI&X\end{pmatrix}$

考虑所有此类有序矩阵对 (A,B)，其中 $(A,B)\in mzjz2\times mzjz2$，再通过 MDS 矩阵的定义，使用程序 5 依次验证 $L=Circ(I\quad I\quad A\quad B)$，其中 $(A,B)\in mzjz2\times mzjz2$，最终得到 2690 个这种形式的 MDS 矩阵，其中 MDS 阵的一行异或数最低为 7，且能够取得 17 个这样的 MDS 矩阵。

例 3：$A_{11}=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&1\\0&1&0&0\end{pmatrix},B_{11}=\begin{pmatrix}0&0&1&0\\1&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$

b) 取 $\begin{cases} A_{11}=A_{22}\in Y\text{为二元域上所有的满秩矩阵} \\ A_{21}=CI, A_{12}=A_{11}^{-1} \end{cases}$，即 $A=\begin{pmatrix} Y & Y^{-1} \\ CI & Y \end{pmatrix}$

考虑所有此类有序矩阵对 (A,B)，其中 $(A,B)\in mzjz2\times mzjz2$，再通过 MDS 矩阵的定义，使用类似程序 5 的程序依次验证：$L=Circ(I\quad I\quad A\quad B)$，其中 $(A,B)\in mzjz2\times mzjz2$ 最终得到 200,072 个这种类型的 MDS 矩阵，其中异或总数最低的 MDS 矩阵共有 12 个，其中 MDS 阵的一行异或数最低为 22。

例 4：$A_{11}=\begin{pmatrix} 0&0&1&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 1&0&0&1 \end{pmatrix}, B_{11}=\begin{pmatrix} 1&0&0&0 \\ 0&0&0&1 \\ 0&1&1&0 \\ 0&0&1&0 \end{pmatrix}$

c) 矩阵 A 满足 $\begin{cases} (A_{12},A_{21})\in One\times One(\text{异或数等于1的所有可逆二元矩阵}), \\ A_{11}=A_{22}=0(0\text{代表零矩阵}) \end{cases}$

即：$A=\begin{pmatrix} 0 & One1 \\ One2 & 0 \end{pmatrix}$

考虑所有此类有序矩阵对 (A,B)，其中 $(A,B)\in mzjz2\times mzjz2$，再通过 MDS 矩阵的定义，依次验证 $L=Circ(I\quad I\quad A\quad B)$，其中 $(A,B)\in mzjz2\times mzjz2$，最终得到 1444 个这种形式的 MDS 矩阵，并且每一个 MDS 矩阵一行的异或数均为 4。

例 5：$A_{12}=\begin{pmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \\ 1&0&0&1 \end{pmatrix}, A_{21}=\begin{pmatrix} 0&0&0&1 \\ 0&1&0&1 \\ 1&0&0&0 \\ 0&0&1&0 \end{pmatrix}$

$$B_{12}=\begin{pmatrix} 0&0&1&1 \\ 1&0&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \end{pmatrix}, B_{21}=\begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&1&1&0 \\ 0&0&0&1 \end{pmatrix}$$

m = 8 时，基于低异或数构造的循环 MDS 矩阵总结如表 1。

2) 基于 4 阶情形的启发式搜索：

通过对 4 阶循环 MDS 矩阵的分析，我们知道形如 $L=Circ(I\quad I\quad A\quad B)$ 这样的异或数最低的 MDS 矩阵满足关系 $A=B^{-2}$ 或 $B=A^{-2}$。为此，考虑如下形式 8 阶矩阵环上的循环型 MDS 矩阵：

$$\begin{pmatrix} I & I & A & A^{-2} \\ A^{-2} & I & I & A \\ A & A^{-2} & I & I \\ I & A & A^{-2} & I \end{pmatrix}$$

Table 1. Cyclic MDS matrix
表 1. 循环 MDS 矩阵

循环矩阵的第一行	生成元来源	特征元素结构	最小异或数
$[I\quad I\quad A\quad B]$	$GL(8,F_2)$	$A_{11}=A_{22}\in X, A_{21}=A_{12}=CI$	28
$[I\quad I\quad A\quad B]$	$GL(8,F_2)$	$A_{11}=A_{22}\in Y, A_{21}=CI, A_{12}=A_{11}^{-1}$	88
$[I\quad I\quad A\quad B]$	$GL(8,F_2)$	$(A_{12},A_{21})\in One\times One, A_{11}=A_{22}=0$	16

为了得到低异或数的矩阵，我们只搜索了 A 是异或数等于 1 的满秩矩阵的情况：记所有八阶异或数为零的满秩矩阵集合为：

$$mzjz0=\left\{A\middle|\#A=0,A\in GL\left(8,F_2\right)\right\}$$

将矩阵 $A\left(A\in mzjz0\right)$ 中的零元素依次用 1 进行替换，得到一个新矩阵，记此变换后的全体矩阵集合为 $mzjz1$，集合中所有矩阵的异或数均为 1，即：

$$mzjz1=\left\{A\middle|\#A=1,A\in GL\left(8,F_2\right)\right\}$$

满足条件的矩阵可从 $mzjz1$ 选取。现检验如下矩阵是否为 MDS 矩阵：

$L=Circ\left(I\quad I\quad A\quad B\right)$，其中 $\left(A,B\right)\in mzjz1\times mzjz1$

使用程序 6 检验，共 96,093 个 MDS 矩阵，其中矩阵异或总数最小为 12，共 80,640 个矩阵满足异或数最小。

例 6：$A=\begin{pmatrix}0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\\0&0&0&0&0&1&0&0\\0&0&0&0&1&0&0&0\\0&0&1&0&0&0&0&0\\0&1&0&0&0&0&0&0\\1&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0\end{pmatrix}$

下面给出一些二元矩阵的性质。

引理 2 [7]：已知 $L=\begin{pmatrix}L_1&L_2\\L_3&L_4\end{pmatrix}$，$L_i\in GL\left(m,F_2\right),1\le i\le 4$，如果 L 的秩为 $2m$，则 $\sum_{i=1}^{4}\#L_i\ge 1$。

证明：假设 $\#L_i=0$，$1\le i\le 4$。则 L_i 的每一行每一列都有一个元素为 1 其中 $1\le i\le 4$。所以 L 是非奇异的，即 $rank\left(L\right)<2m$，矛盾。证毕。

定理 1：1) 若 $L=Circ\left(A,B,C,D\right)$ 是一个循环的 MDS 矩阵，其中 $A,B,C,D\in GL\left(m,F_2\right)$，则 $\#A+\#B+\#C+\#D>2$；2) 若 $L=Had\left(A,B,C,D\right)$ 是一个 *Hadamard* MDS 矩阵，其中 $A,B,C,D\in GL\left(m,F_2\right)$，则 $\#A+\#B+\#C+\#D>3$。

证明：1) 设 $L=Circ\left(A,B,C,D\right),A,B,C,D\in GL\left(m,F_2\right)$ 是一个循环的 MDS 矩阵。

若 $\#A+\#B+\#C+\#D\le 1$，则在第一行中至少含有三个异或数为 0，不妨假设 $\#A=\#B=\#C=0$，有 $rank\left(L\left(\left[1\ 2\right],\left[2\ 3\right]\right)\right)=rank\left(\begin{pmatrix}B,C\\A,B\end{pmatrix}\right)<2m$，因 L 是一个 MDS 矩阵，所以这与假设矛盾。其他情况同样可以被证明。

若 $\#A+\#B+\#C+\#D=2$，则对某一行至少有两个元素异或数为零，其余两个元素异或数之和为 2。

当 $m=4$ 时：

a) 不妨设 $\#A=\#B=1,\#C=\#D=0$。采用如下搜索策略：当 $m=4$ 时，首先得到一个包含所有异或数为 1 的满秩矩阵的集合 *One* 以及包含所有异或数为 0 的满秩矩阵的集合 $Z0$，然后对每一个数组 $\left(A,B,C,D\right)\in One\times One\times Z0\times Z0$，带入检验 $Circ\left(A\quad B\quad C\quad D\right)$ 是否为 MDS 矩阵，通过运行程序 1，并未检测到任何满足条件的矩阵；

b) 不妨设 $\#A=2,\#B=\#C=\#D=0$，记异或数为零的矩阵集合为 I_0，则

$$L = Circ(A,B,C,D) = \begin{pmatrix} A & B & C & D \\ D & A & B & C \\ C & D & A & B \\ B & C & D & A \end{pmatrix}, B,C,D \in I_0,$$

显见 L 存在一个子方阵 $L([1,2],[3,4]) = \begin{pmatrix} C & D \\ B & C \end{pmatrix}$, $rank\left(L([1,2],[3,4])\right) = 0$，

$rank\left(L([1,2],[3,4])\right) = 0$，此时的 L 一定不是 MDS 矩阵。

当 $m = 8$ 时，同理可证，详见附件程序 2。

由矩阵的初等行列变换知，交换上述 $A\ B\ C\ D$ 的位置不会影响 $Circ(A\quad B\quad C\quad D)$ 的 MDS 性，故该证明具有一般性。

综上可得，满足 $\#A+\#B+\#C+\#D>2$

2) $L = Had(A,B,C,D)$ 是一个 *Hadamard* MDS 矩阵。

若 $\#A+\#B+\#C+\#D \le 2$，则在第一行中至少含有两个异或数为 0，不失普遍性，这里假设 $\#A=\#C=0$，据引理 2，有 $rank\left(L([1\ 3],[1\ 3])\right) = rank\left(\begin{pmatrix} A,C \\ C,A \end{pmatrix}\right) < 2m$，因 L 是一个 MDS 矩阵，所以这与假设矛盾。其他情况同样可以被证明。

若 $\#A+\#B+\#C+\#D=3$，则对某一行至少有一个元素异或数为零，其余三个元素异或数之和为 3。

当 $m = 4$ 时：

1) 不妨设 $\#A=\#B=\#C=1,\#D=0$，采用如下搜索策略：首先可记一个包含所有异或数为 1 的满秩矩阵的集合 *One* 和包含所有异或数为 0 的满秩矩阵 $Z0$。然后对每一个数组 $(A,B,C,D) \in One\times One\times One\times Z0$，带入程序 3 的 findMDS1.m 检验是否为 MDS 矩阵的程序中，通过运行程序，并未检测到任何满足条件的矩阵。

2) 不妨假设 $\#A=2,\#B=1,\#C=\#D=0$，搜索策略如下：记一个包含所有异或数为 1 的矩阵的集合 *One*，一个包含所有异或数为 2 的矩阵的集合 *Two*。然后对每一个数组 $(A,B,C,D) \in Two\times One\times Z0\times Z0$，带入程序 3 中的 findMDS2.m 检验是否为 MDS 矩阵的程序中，通过运行程序，并未检测到任何满足条件的矩阵。

3) 假设 $\#A=3$，$\#B=\#C=\#D=0$，$L = Had(A\quad B\quad C\quad D) = \begin{pmatrix} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{pmatrix}, B,C,D \in I_0$。

显见 L 存在一个子方阵 $L([1,2],[3,4]) = \begin{pmatrix} C & D \\ D & C \end{pmatrix}$，显然 $rank\left(L([1,2],[3,4])\right) = 0$，所以此时的 L 一定不是 MDS 矩阵。

当 $m = 8$ 时，同理可证。

由矩阵的初等行列变换知，交换上述 $A\ B\ C\ D$ 的位置不会影响 $Circ(A\quad B\quad C\quad D)$ 的 MDS 性，故该证明具有一般性。

综上，$L = Had(A,B,C,D)$ 是一个 MDS 矩阵，则 $\#A+\#B+\#C+\#D>3$。证毕。

利用上述定理知 4 阶或 8 阶矩阵环上的循环型 MDS 矩阵异或数不小于 12。前面构造说明异或数 12 是可以达到的，并已经取得。

2.2. 循环 MDS 矩阵的改进

此节继续考虑特殊分块矩阵，尝试构造类似循环矩阵的 MDS 矩阵，记循环矩阵为 $L=Circ\left(A\quad B\quad C\quad D\right)$，考虑类似循环矩阵的矩阵：

$L_0=\begin{pmatrix}A & B & C & D\\ D & A & B & C\\ C & D & A & B\\ B & C & D & E\end{pmatrix}$，其中 $A,B,C,D,E\in GL\left(4,F_2\right)$

对这类矩阵，期望得到异或数低于 12 的 MDS 矩阵。

对已知异或总数为 12 的循环 MDS 矩阵的分析，发现总是可以表示成 $A=B^{-2}$ 或者 $B=A^{-2}$ 其中 $A\quad B$ 的异或数为 1，$A^{-2}\quad B^{-2}$ 的异或数为 2。现在对 24 对矩阵序对 $\left(A\quad A^{-2}\right)$ 中异或数为 2 的矩阵进行替换，即将某一个 A^{-2} 替换为集合 One 中的元素。其中：$One=\left\{A\in GL\left(4,F_2\right)\middle|\#A=1\right\}$

考虑 $L_0=\begin{pmatrix}I & I & A & B\\ B & I & I & A\\ A & B & I & I\\ I & A & C & I\end{pmatrix},C\in One$。

很遗憾，使用程序 7 搜索并没有异或数小的 MDS 矩阵的出现。

2.3. 轻量级 Hadamard 型 MDS 矩阵的构造

记 L_0 为 *Hadamard* 循环矩阵：

$$L_0=Had\left(A,B,C,D\right)=\begin{pmatrix}A & B & C & D\\ B & A & D & C\\ C & D & A & B\\ D & C & B & A\end{pmatrix},\text{其中}A,B,C,D\in GL\left(m,F_2\right),m=4,8$$

要想 $Had\left(A,B,C,D\right)$ 为 MDS 矩阵，则至少要求下列矩阵是满秩矩阵：

$$A+BA^{-1}B,B+AD^{-1}C,C+DC^{-1}D,B+AD^{-1}C,B+DC^{-1}A$$

通过分析，若是采用全局程序搜索，当 $m=4$ 和 8 时程序运算量太大，故不实际，由此需要对 A,B,C,D 进行特殊处理。

当 $m=4$ 时考虑如下三种特殊 Hadamad 矩阵：

1) 令 $L_0=Had\left(I,A,I,B\right),A,B\in GL\left(4,F_2\right)$。要使得 L_0 为 MDS 矩阵，则下列矩阵一定为满秩矩阵：

$$A^2+I,B^2+I,A+B,AB+I,A^2+B^2$$

使用程序 8 来搜索满足条件的此类 MDS 矩阵，发现此类 MDS 矩阵不存在。

2) 令 $L_0=Had\left(I,A,A,B\right)$，即 $Had\left(I,A,A,B\right)=\begin{pmatrix}I & A & A & B\\ A & I & B & A\\ A & B & I & A\\ B & A & A & I\end{pmatrix}$，其二阶子方阵中

存在 $rank\left(L_0\left(\left[2,3\right],\left[1,4\right]\right)\right)=0$。程序发现不存在此类 MDS 矩阵。

3) 令 $L_0=Had\left(I,A,A^{\mathrm{T}},B\right)$。若 $L_0=Had\left(I,A,A^{\mathrm{T}},B\right)$ 为 MDS 矩阵，则要求下列矩阵一定为满秩矩阵：

$$A+I,A^{\mathrm{T}}+I,B+I,AA^{\mathrm{T}}+B,A^{\mathrm{T}}A+B,AB+A^{\mathrm{T}},BA+A^{\mathrm{T}},A^{\mathrm{T}}B+A,BA^{\mathrm{T}}+A$$

使用程序得到 $Had\left(I,A,A^{\mathrm{T}},B\right)$ 型的 MDS 矩阵共有 7917 个，其中矩阵一行的最低异或数为 4，并且，给出了 48 组这样的矩阵对 (A,B) 使得 $L_0=Had\left(I,A,A^{\mathrm{T}},B\right)$ 为 MDS 矩阵，且满足 $\#A+\#A^{\mathrm{T}}+\#B=4$。

例 7：$A=\begin{pmatrix}0&0&0&1\\0&0&1&0\\1&0&0&0\\1&1&0&0\end{pmatrix},B=\begin{pmatrix}0&0&1&0\\0&0&1&1\\1&1&0&0\\0&1&0&0\end{pmatrix}$

将这几种情形 Hadamard 矩阵总结如表 2。

显见，此时得到的 MDS 矩阵异或总数并不是所有矩阵中最小的，与目标还有一定的距离。为此，考虑如何改进我们的矩阵，从而得到更优结果，还有待进一步的研究。

当 $m=8$ 时，考虑满足如下条件的 Hadamard 矩阵：

将 L_0 中所有非单位元的元素均拆分为如下形式：

$$mzjz2=\left\{A\middle|A=\begin{pmatrix}A_{11}&A_{12}\\A_{21}&A_{23}\end{pmatrix},\text{其中}A_{ij}\in GL\left(4,F_2\right)\text{且}rand\left(A\right)=8\right\}$$

再次对矩阵 A 的异或数做限定，令集合

$$zxors2=\left\{A\middle|\#A\le 2,\text{其中}A\in GL\left(m,F_2\right),m=4,8\right\}$$

构造这样的 $A_{ij},B_{ij}\in zxors2$，满足 $\begin{cases}A_{11}=A_{22}=0\\A_{12}=A_{21}\left(\text{满秩}\right)\end{cases},\begin{cases}B_{11}=B_{22}=0\\B_{12}=B_{21}\left(\text{满秩}\right)\end{cases}$，使用类似程序搜索得到了形如 $Had\left(I,A,A^{\mathrm{T}},B\right)$ 的 MDS 矩阵有 6693 个，且矩阵异或总数最小为 32，共有 48 个矩阵能够取得最小异或总数。

例 8：$A_{12}=\begin{pmatrix}0&0&0&1\\0&0&1&0\\1&0&0&0\\1&1&0&0\end{pmatrix},B_{12}=\begin{pmatrix}0&0&1&0\\0&0&1&1\\1&1&0&0\\0&1&0&0\end{pmatrix}$

令集合 $zxors1=\left\{A\middle|\#A\le 1\right\}$，先取定 $A\in zxors1,B\in zxors2$。检验此时的 $Had\left(I,A,A^{\mathrm{T}},B\right)$ 是否为 MDS 矩阵，没有任何结果返回。这说明当 $\#A\le 1,\#B\le 2$ 时，根本不存在 $Had\left(I,A,A^{\mathrm{T}},B\right)$ 型 MDS 矩阵。由此有如下定理。

定理 2：已知 $A,B\in GL\left(4,F_2\right)$，如果 $Had\left(I,A,A^{\mathrm{T}},B\right)$ 矩阵是 MDS 矩阵，则一定有 $\#A+\#A^{\mathrm{T}}+\#B\ge 4$。

2.4. 最佳 MDS 矩阵的构造

文献[8]构造了一类 MDS 矩阵：

Table 2. Hadamard MDS matrix
表 2. Hadamard MDS 矩阵

矩阵类型	生成元来源	MDS 矩阵个数	最小异或数
$Had\left(I,A,I,B\right)$	$GL\left(4,F_2\right)$	/	/
$Had\left(I,A,A,B\right)$	$GL\left(4,F_2\right)$	/	/
$Had\left(I,A,A^{\mathrm{T}},B\right)$	$GL\left(4,F_2\right)$	7917	16

$$\begin{pmatrix} a & 1 & 1 & 1 \\ 1 & 1 & b & a \\ 1 & a & 1 & b \\ 1 & b & a & 1 \end{pmatrix}$$

文献[8]中被称为最佳矩阵。基于这个思想，本小节研究如下矩阵：

$$L = \begin{pmatrix} A & I & I & I \\ I & I & B & A \\ I & A & I & B \\ I & B & A & I \end{pmatrix}$$

要求 L 为 MDS 矩阵，则必有以下矩阵是满秩矩阵：

$$A+I, A^2+I, B+I, A+B, A+B^2, A^2+B, AB+I$$

当 $m = 4$ 时，考虑满足条件的 A,B，使用程序 9 得到共 48878 个最佳 MDS 矩阵，其中存在 43 组满足条件的矩阵对 (A,B)，使得最佳 MDS 矩阵的异或数达到最小为 13，即 $4\#A+3B=13$，经观察，这些矩阵中的矩阵对 (A,B) 均满足 $B=A^{-2}$，其中 $\#A=1, \#A^{-2}=3$。

例 9：$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

当 $m = 8$ 时，考虑 $GL(8, F_2)$ 中满足条件的 A,B，基于 $m = 4$ 时得到的结论，为找到异或数较低的 MDS 矩阵，不妨尝试令 $B = A^{-2}$，考虑二元域上所有异或数等于 1 的满秩矩阵，使用程序 10，检验得到 61,528 个 MDS 矩阵，其中 40320 个异或数为 10 的最佳 MDS 矩阵。

例 10：$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$

2.5. 利用迭代寻找轻量级 MDS 矩阵

构造 MDS 矩阵可以利用有限域以及 MDS 码，除此以外，最常用的方法还有迭代法。迭代法的主要思想是通过利用较小分支数的扩散层重复作用，最终得到具有最大分支数的扩散层。实施此方法的第一步并不是构造一个 MDS 矩阵，这种新的设计策略在轻量级的哈希函数中被提出[9]，例如 PHOTON 算法，在 LED 轻量分组密码的设计中被大量应用[10]。典型的代表是利用线性反馈移位寄存器的构造。使用此方法，本小节中构造一些具有低异或数的 MDS 矩阵。

记 LFSR MDS 矩阵 L 具有如下形式：

$$L(A \quad B \quad C \quad D) = \begin{pmatrix} 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ A & B & C & D \end{pmatrix}$$

Table 3. Lightweight MDS Matrix
表 3. 轻量级 MDS 矩阵

形式	d 的范围	最小异或总数	MDS 矩阵总个数
$L(A^{-2} \quad I \quad I \quad A^{-2})$	4~100	51	14,853
$L(A \quad I \quad I \quad A^{-2})$	4~100	35	22,951
$L(A \quad I \quad I \quad A^{-1})$	4~100	35	2733
$L(I \quad I \quad I \quad A^{-1})$	4~100	41	21,575
$L(A^{3} \quad I \quad A^{-3} \quad A^{2})$	4~100	39	16,197
$L(A^{4} \quad I \quad A^{-4} \quad A^{-3})$	4~100	24	16,185
$L(A^{4} \quad I \quad A^{-5} \quad A^{-4})$	4~100	42	20,211

其中$(A \quad B \quad C \quad D) \in GL(m, F_2), m = 4,8$。由矩阵 L 迭代生成 MDS 矩阵时，迭代次数不超过 100 次。为了减少程序搜索量，考虑矩阵 $L(A \quad B \quad C \quad D)$ 中每一行的元素至多有两个不相关的变量。文献[9]考虑矩阵 $L(A \quad I \quad I \quad A^2)$，其中 $A \in GL(m, F_2)$，可通过合适的线性变换得到一个 MDS 矩阵。不妨就取定 $L = L(A \quad I \quad I \quad A^2)$，其中 $A \in GL(m, F_2)$

当 $m = 4$ 时，考虑 $GL(4, F_2)$ 上的所有二元矩阵，然后将矩阵 L 带入进行运算，得到所有的矩阵(注意：此处假设迭代 100 次)。利用 MDS 矩阵的定义，使用程序 11 找出迭代后的所有 MDS 矩阵，总共得到 18,882 个 MDS 矩阵，其中具有最小异或数的矩阵有 24 个，这些矩阵的异或总数为 42。此时的迭代次数 d 可以取到 82。

例 11：$A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, d = 82$

此时通过该形式迭代得到的 MDS 矩阵异或数不是很理想。虽然在 $L(A \quad I \quad I \quad A^2)$ 中我们并没有找到轻量级的 MDS 矩阵，但是通过修改生成元及其形式，有望得到异或数较小的 MDS 矩阵。使用以上的搜索策略，尝试了多种形式，均有 MDS 矩阵的返回，现将结果列于表 3。

3. 总结

本文考虑具有小的异或数 MDS 矩阵的构造，使用循环、分块和迭代等思想来考虑 MDS 矩阵，分析 MDS 矩阵的性质，考虑特殊情况下的矩阵，分别对几种情况的特殊矩阵，在 m = 4 和 8 下，使用程序搜索，得到这些 MDS 矩阵的异或数最小的情况，并计数和给出相关例子。如何构造最小的异或数的 MDS 矩阵是一个有趣和实际应用的问题，需要进一步研究。

基金项目

本文得到四川省科技厅 2015 年第一批科技计划项目(基本科研-重点研发) (2015JY0245)、四川省教育厅自然科学重点项目(15ZA0135)，在此表示感谢！

参考文献

[1] Daemen, J. and Rijmen, V. (2001) The Wide Trail Design Strategy. *Proceedings of the* 8*th IAM international Conference*, Springer-Verlag, Berlin, Volume 2260: 222-238.

[2] Daemen, J. and Rijmen, V. (2002) The Design of Rijndael: AES—The Advanced Encryption Standard. Springer

Science & Business Media. https://doi.org/10.1007/978-3-662-04722-4

[3] Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A. and De Win, E. (1996) The cIpher SHARK. In: *Fast Software Encryption*. Vol. 1039 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, 99-111. https://doi.org/10.1007/3-540-60865-6_47

[4] Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. and Ferguson, N. (1998) Twofish: A 128-Bitblock Cipher. NIST AES Proposal, 15. http://dblp.uni-trier.de/db/conf/rsfdgrc/index.html

[5] Barreto, P. and Rijmen, V. (2000) The Khazad Legacy-Level Block Cipher. Submission to the Nessie Project, 97. http://dblp.uni-trier.de/db/conf/rsfdgrc/index.html

[6] Guo, J., Peyarin, T. and Poschmann, A. (2011) The PHOTON Family of Lightweight Hash Function. *CRYPTO*'11, Springer-Verlag, Berlin, Volume 6841: 222-239.

[7] Li, Y. and Wang, M. (2016) On the Construction of Lightweight Circulant Involutory MDS Matrices. FSE 2016. IACR Cryptology ePrint Archive, 2016: 406. http://eprint.iacr.org/

[8] Junod, P. and Vaudenay, S. (2004) Perfect Diffusion Primitives for Block Ciphers Building Efficient MDS Matrices. In: Handschuh, H. and Hasan, M.A., Eds., *SAC* 2004. LNCS, Volume 3357, 84-99. Springer, Heidelberg.

[9] Wu, S., Wang, M. and Wu, W. (2012) Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions. In: Knudsen, L.R. and Wu, H., Eds., *SAC* 2012: *Selected Areas in Cryptography*, LNCS, Volume 7707, 355-371. https://doi.org/10.1007/978-3-642-35999-6_23

[10] Guo, J., Peyrin, T., Poschmann, A. and Robshaw, M. (2011) The LED Block Cipher. In: Preneel, B. and Takagi, T., Eds., *CHES* 2011: *Cryptographic Hardware and Embedded Systems*, LNCS, Volume 6917, 326-341. Springer, Heidelberg. https://doi.org/10.1007/978-3-642-23951-9_22

附录(主要程序)

程序 1：

1、

```
%测试矩阵 X 是否为 MDS 矩阵，若是则返回 1，否则返回 0
%被检测矩阵必须为方阵且其阶数必须为 4 的倍数
function y=ismds(x)
n1=size(x);
n=n1(1);
m=n/4;
y=1;
%检查全矩阵
if ~ismz(x)
    y=0;
    return
end
%检查 1 阶子方阵
for i=1:4
    for j=1:4
        if
~ismz(x([1:4]+4*(i-1),[1:4]+4*(j-1)))
            y=0;
            return
        end
    end
end

%检查 2 阶子方阵
for i1=1:3
    for i2=i1+1:4
        for j1=1:3
            for j2=j1+1:4
                if
~ismz(x([[1:4]+4*(i1-1);[1:4]+4*(i2-1)],[[1:4]
+4*(j1-1),[1:4]+4*(j2-1)]))
                    y=0;
                    return
                end
            end
        end
    end
end
%检查 3 阶子方阵
for i=1:4
    for j=1:4
        a=[1:4]+4*(i-1);
        b=[1:4]+4*(j-1);
        c=1:16;
        d=c;
        c(a)=[];
        d(b)=[];
        if ~ismz(x(c,d))
            y=0;
            return
        end
    end
end
```

2、

```
clear
clc
load('z0.mat')
load('one.mat')
k=0;
for i=1:288
    for j=1:288
        for k=1:24
            for n=1:24
                if
ismds(circ(one{i},one{j},z0{k},z0{n}))

circ(one{i},one{j},z0{k},z0{n})
                end
            end
        end
    end
    i
end
```

程序 2：

1、

```
clear
clc
load('mzjz0.mat')
load('mzjz1.mat')
k=0;
for i=1:2257920
    for j=1:2257920
        for k=1:40320
            for n=1:40320
                if
ismds(circ(mzjz1{i},mzjz1{j},mzjz0{k},mzjz0
{n}))
```

```
circ(mzjz1{i},mzjz1{j},mzjz0{k},mzjz0{n})
                        end
                    end
                end
            end
        i
end
```

2、

```
clear
clc
load('z0.mat')
load('one.mat')
k=0;
for i=1:288
    for j=1:288
        for k=1:228
            for n=1:24
                if
ismds(had(one{i},one{j},one{k},z0{n}))

had(one{i},one{j},one{k},z0{n})
                        end
                    end
                end
            end
        i
end
```

3、

```
clear
clc
load('z0.mat')
load('one.mat')
load('two.mat')
k=0;
for i=1:1440
    for j=1:288
        for k=1:24
            for n=1:24
                if
ismds(had(two{i},one{j},z0{k},z0{n}))

had(two{i},one{j},z0{k},z0{n})
                        end
                    end
                end
            end
        i
end
```

程序 3：

1、

```
%检验由 ab 生成的循环矩阵是否是 MDS 矩阵并求
异或数
clear
load('ab.mat')
n=size(ab);
k=1;
for i=1:n(2)
    a=circ(eye(4,4),eye(4,4),ab{1,i},ab{2,i});
    if ismds(a)
        mds4{1,k}=ab{1,i};
        mds4{2,k}=ab{2,i};

mds4{3,k}=4*(xors(ab{1,i})+xors(ab{2,i}));
        k=k+1;
    end
end
```

2、

```
%     k=1;
%for i=1:370944
%     if mds4{3,i}==12
%         s(k)=i
%         k=k+1
%     end
%end
for i=1:48
    mds4s{1,i}=mds4{1,s(i)};
    mds4s{2,i}=mds4{2,s(i)};
end
```

程序 4：

1、

```
%检验由 ab 生成的循环矩阵是否是 MDS 矩阵并求
异或数
clear
load('ab.mat')
n=size(ab);
k=1;
for i=1:n(2)
    a=circ(eye(4,4),eye(4,4),ab{1,i},ab{2,i});
    if ismds(a)
        mds4{1,k}=ab{1,i};
        mds4{2,k}=ab{2,i};

mds4{3,k}=4*(xors(ab{1,i})+xors(ab{2,i}));
        k=k+1;
```

```
        end
    end
    2、
    %生成 mds8
    %clear
    %load('x.mat')
    n1=size(x);
    n=n1(2);
    k=0;
    for i=1:n
        for j=1:n
            y=circ(eye(8),eye(8),x{i},x{j});
            %y=had((x{j})',x{i},x{i}',x{j});
            if ismds(y)
                k=k+1
                mds8{k}=y;
            end
        end
        i
    end
```

程序 6：

```
    1、
    clear
    clc
    load('mzjz1.mat')
    n1=size(mzjz1);
    n=n1(2);
    k=0;
    for i=1:n
        x=mzjz1{i};
        y=circ(eye(8),eye(8),x,ccf(qn(x),2));
        if ismds(y)
            k=k+1
            mds8c{k}=y;
            xx(k)=zxors(y);
        end
    end
    2、
    %搜索 mds 矩阵
    %clear
    %load('ab.mat')
    n1=size(ab);
    n=n1(2);
    k=0;
    for i=1:n
        if
    ismds(had(eye(4),ab{1,i},ab{1,i}',ab{2,i}))
            k=k+1

    mds4{k}=had(eye(4),ab{1,i},ab{1,i}',ab{2,i});
            i
        end
    end
    3、
    clear
    clc
    load('ab.mat')
    k=0;
    for i=1:370944
        a=ab{1,i};
        b=ab{2,i};
        if ismds(opt(a,b))
            k=k+1;
            mds4o{1,k}=opt(a,b);
            mds4o{2,k}=a;
            mds4o{3,k}=b;
        end
    end


    4、
    clear
    clc
    load('mzjz1.mat')
    n1=size(mzjz1);
    n=n1(2);
    k=0;
    for i=1:n
        x=mzjz1{i};
        y=opt(x,ccf(qn(x),2));
        if ismds(y)
            k=k+1
            mds8o{k}=y;
            xx(k)=zxors(y);
        end
    end
```

程序 7：

```
    1、
    clear
    load('mzjz.mat')
    n1=size(mzjz);
    n=n1(2);
    k=1;
    for i=1:n
```

```
x=lfsr(ccf(mzjz{i},4),eye(4),ccf(qn(mzjz{i}),3
),ccf(qn(mzjz{i}),2));
    y=ccf(x,4);
    for j=4:100
        if ismds(y)
            mds{1,k}=mzjz{i};
            mds{2,k}=j;
            k=k+1;
        end
        y=cf(x,y);
    end

end
```

2、

```
clear
load('mzjz.mat')
n1=size(mzjz);
n=n1(2);
k=1;
for j=4:100
    for i=1:n

x=lfsr(eye(4),eye(4),eye(4),qn(mzjz{i}));
        y=ccf(x,j);
        if ismds(y)
            mds4{1,k}=mzjz{i};
            mds4{2,k}=j;
            k=k+1
        end
    end
    j
end
```

程序 7：

1、

```
%搜索 mds 矩阵
%clear
%load('ab.mat')
n1=size(ab);
n=n1(2);
k=0;
for i=1:n
    if
ismds(had(eye(4),ab{1,i},ab{1,i}',ab{2,i}))
        k=k+1

mds4{k}=had(eye(4),ab{1,i},ab{1,i}',ab{2,i});
        i
    end
End
```

程序 9：

1、

```
clear
clc
load('ab.mat')
k=0;
for i=1:370944
    a=ab{1,i};
    b=ab{2,i};
    if ismds(opt(a,b))
        k=k+1;
        mds4o{1,k}=opt(a,b);
        mds4o{2,k}=a;
        mds4o{3,k}=b;
    end
end
```

程序 10：

1、

```
clear
clc
load('mzjz1.mat')
n1=size(mzjz1);
n=n1(2);
k=0;
for i=1:n
    x=mzjz1{i};
    y=opt(x,ccf(qn(x),2));
    if ismds(y)
        k=k+1
        mds8o{k}=y;
        xx(k)=zxors(y);
    end
end
```