• 安全技术 • 文章编号：1000—3428(2013)12—0118—04 文献标识码：A 中图分类号：TP309

一类具有最大分支数的 16 阶 0-1 矩阵构造

郭 磊[1]，郑浩然[1]，刘明伟[2]

(1. 解放军信息工程大学三院，郑州 450004；2. 空军西安飞行学院，西安 710300)

摘 要：具有最大分支数的 0-1 可逆矩阵被广泛应用于分组密码的扩散结构设计中。为构造 16 阶该类矩阵，将 16 阶 0-1 矩阵划分为以 4 阶 0-1 矩阵为单元的 4 阶块矩阵，根据特征和域上重量均为 2 的 4 维 0-1 向量相加后所得向量的重量分布特点，在行置换同构意义下构造满足某种特殊结构的 4 阶 0-1 矩阵单元组，以此为基础，根据 Hadamard 矩阵的结构特点，利用矩阵的分块构造思想，给出一类分支数达到最大值 8 的 16 阶 0-1 可逆矩阵和对合矩阵构造方法，并在行置换同构意义下给出对合矩阵的计数。

关键词：分组密码；扩散结构；分支数；0-1 矩阵；Hadamard 矩阵

Construction of a 16×16 0-1 Matrice with Maximum Branch Number

GUO Lei[1], ZHENG Hao-ran[1], LIU Ming-wei[2]

(1. The 3rd Institute, PLA Information Engineering University, Zhengzhou 450004, China;
2. The Air Force Xi'an Flight Academy, Xi'an 710300, China)

【Abstract】0-1 invertible matrice which has the largest branch number is widely used in the design of diffusion structures in block ciphers. In view of how to construct such 16×16 matrix, this paper divides 16×16 matrix into 4×4 block matrix by 4×4 0-1 matrix as a unit. Using the weight distribution peculiarity of the sum of 4-dimensional 0-1vectors with weight 2 in field of characteristic 2, it constructs 4×4 0-1 matrix unit group with some special structures in the permutation of isomorphism. On the basis of the structure characteristic of Hadamard matrice, it presents the methods of constructing 16×16 invertible 0-1 matrice with maximum branch number 8 using the matrix block construction method. Further, it presents the methods of constructing 16×16 involutory 0-1 matrice with maximum branch number 8 and their number in the permutation of isomorphism.

【Key words】block cipher; diffusion structure; branch number; 0-1 matrice; Hadamard matrice

DOI: 10.3969/j.issn.1000-3428.2013.12.025

1 概述

混乱原则和扩散原则是保证分组密码安全性的 2 个基本设计原则。在分组密码中，其扩散特性往往是通过特定的扩散结构来实现的，扩散结构的设计非常重要，直接关系到分组密码的安全性能和实现性能[1-2]。

分支数理论是分组密码扩散结构设计的一个重要理论，设计者可以根据分支数的大小从理论上给出最大差分特征概率和最佳线性逼迫优势的界，从而保证分组密码对差分密码分析和线性密码分析是实际安全的[3-4]。

以分支数尽可能大的线性变换作为分组密码算法的扩散结构是设计分组密码的一种重要方法，线性变换的构造可通过可逆矩阵的构造完成。由于 0-1 矩阵软、硬件实现速度快并且占用资源少的特点，使得 0-1 矩阵在分组密码扩散结构的设计中得到广泛应用，如 Camellia[5]、E2[6]、ARIA[7]等算法均采用了 8 阶或 16 阶 0-1 矩阵来设计其扩散结构。因此如何构造具有最大分支数的 0-1 矩阵成为分组密码研究的热点问题。文献[8]指出 8 阶和 16 阶 0-1 矩阵的最大分支数分别为 5 和 8，并且当 0-1 矩阵的差分分支数达到最大时，其线性分支数也达到最大，反之亦然。文献[9]对分支数为 5 的 8 阶 0-1 矩阵的结构进行了研究，给出了构造所有分支数为 5 的 8 阶 0-1 矩阵的方法。文献[10]给出了分支数为 5 的一类 8 阶 0-1 矩阵的构造方法，并在循环矩阵中搜索出了大量的分支数为 8 的 16 阶 0-1 矩阵。文献[11]基于极大距离可分码给出了一种构造分支数为 8 的 16 阶非对合的 0-1 矩阵的方法。

根据特征为 2 的域上 4 阶 0-1 矩阵和 4 阶 Hadamard 矩阵的结构和性质，本文针对输入输出均为 16 块的扩散结构，对分支数为 8 的 16 阶 0-1 矩阵进行研究，给出一类分支数为 8，各行各列重量都为 7 的 16 阶 0-1 可逆矩阵构造方法，

基金项目：国家自然科学基金资助项目(61272041)

作者简介：郭 磊(1986－)，男，硕士研究生，主研方向：密码学；郑浩然，副教授；刘明伟，助理工程师

收稿日期：2012-10-26 **修回日期：**2013-01-06 **E-mail：**gl200644@163.com

进而给出一类分支数为 8，各行各列重量都为 7 的 16 阶 Hadamard 型对合 0-1 矩阵构造方法，并且在矩阵行置换同构的意义下给出其计数。

2　基础知识

定义 1 设 $\boldsymbol{A}$ 为 n 阶 0-1 矩阵，则：

$$\beta(\boldsymbol{A})=\min\{w(\boldsymbol{x})+w(\boldsymbol{A}\boldsymbol{x}^{\mathrm{T}})\mid \boldsymbol{x}\in(\{0,1\}^m)^n,\boldsymbol{x}\neq\boldsymbol{0}\}$$

称为 0-1 矩阵 $\boldsymbol{A}$ 的分支数。其中，$w(\boldsymbol{x})$ 表示 $\boldsymbol{x}$ 的重量[9]。

定义 2 设 $\boldsymbol{A}$、$\boldsymbol{B}$ 为 2 个 0-1 矩阵，若存在行置换 ρ 和列置换 γ，使得 $\rho(\gamma(\boldsymbol{A}))=\gamma(\rho(\boldsymbol{A}))=\boldsymbol{B}$，那么称 0-1 矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是置换同构的[9]。

引理 1 若 0-1 矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是置换同构的，那么 $\beta(\boldsymbol{A})=\beta(\boldsymbol{B})$ [9]。

定义 3 $a_0,a_1,\cdots,a_{n-1}$ 是特征为 2 的域中的 n 个元，若矩阵 $\boldsymbol{A}=(a_{i,j})_{i,j=0}^{n-1}$，$a_{i,j}=a_{i\oplus j}$，则称 $\boldsymbol{A}$ 是一个由 a_0，$a_1,\cdots,a_{n-1}$ 决定的 Hadamard 矩阵[12]。

引理 2 若特征为 2 的域上的 $\boldsymbol{A}$ 是由 $a_0,a_1,\cdots,a_{n-1}$ 决定的一个 n 阶 Hadamard 矩阵，则 $\boldsymbol{A}^2=\gamma\cdot\boldsymbol{E}$，$\gamma=\bigoplus_{i=0}^{n-1}a_i^2$ [12]。

在特征为 2 的域上，重量为 2 的 4 维 0-1 列向量共有 6 个，分别为：

$$(1\ \ 1\ \ 0\ \ 0)^{\mathrm{T}},(0\ \ 0\ \ 1\ \ 1)^{\mathrm{T}},(1\ \ 0\ \ 0\ \ 1)^{\mathrm{T}}$$
$$(0\ \ 1\ \ 1\ \ 0)^{\mathrm{T}},(1\ \ 0\ \ 1\ \ 0)^{\mathrm{T}},(0\ \ 1\ \ 0\ \ 1)^{\mathrm{T}}$$

如果令 $\boldsymbol{\alpha}_0=(1\ \ 1\ \ 0\ \ 0)^{\mathrm{T}}$，$\boldsymbol{\alpha}_1=(1\ \ 0\ \ 0\ \ 1)^{\mathrm{T}}$，$\boldsymbol{\alpha}_2=(1\ \ 0\ \ 1\ \ 0)^{\mathrm{T}}$，$\bar{\boldsymbol{\alpha}}$ 为 $\boldsymbol{\alpha}$ 的补向量，则上述 6 个列向量即为：$\boldsymbol{\alpha}_0,\bar{\boldsymbol{\alpha}}_0,\boldsymbol{\alpha}_1,\bar{\boldsymbol{\alpha}}_1,\boldsymbol{\alpha}_2,\bar{\boldsymbol{\alpha}}_2$。那么各行各列重量均为 2 的 4 阶 0-1 矩阵行置换同构于 $(\boldsymbol{\alpha}_i,\bar{\boldsymbol{\alpha}}_i,\boldsymbol{\alpha}_j,\bar{\boldsymbol{\alpha}}_j)$，$0\leqslant i,j\leqslant 2$，并有如下的结论：

定理 1 各行各列重量都为 2 的 3 个 4 阶 0-1 矩阵 $\boldsymbol{A}_i=(\boldsymbol{a}_{i0},\boldsymbol{a}_{i1},\boldsymbol{a}_{i2},\boldsymbol{a}_{i3}),i=0,1,2$，如果矩阵 $(\boldsymbol{A}_{i_1}^{\mathrm{T}},\boldsymbol{A}_{i_2}^{\mathrm{T}},\boldsymbol{A}_{i_3}^{\mathrm{T}})^{\mathrm{T}}$ 行置换同构于 $\begin{pmatrix}\boldsymbol{\alpha}_{j_0},\boldsymbol{\alpha}_{j_0},\bar{\boldsymbol{\alpha}}_{j_0},\bar{\boldsymbol{\alpha}}_{j_0}\\ \boldsymbol{\alpha}_{j_1},\bar{\boldsymbol{\alpha}}_{j_1},\boldsymbol{\alpha}_{j_1},\bar{\boldsymbol{\alpha}}_{j_1}\\ \boldsymbol{\alpha}_{j_2},\bar{\boldsymbol{\alpha}}_{j_2},\bar{\boldsymbol{\alpha}}_{j_2},\boldsymbol{\alpha}_{j_2}\end{pmatrix}$，则对任意互不相等的 k 和 l，$0\leqslant k,l\leqslant 3$，则：

$$w(\boldsymbol{a}_{0k}\oplus\boldsymbol{a}_{0l})+w(\boldsymbol{a}_{1k}\oplus\boldsymbol{a}_{1l})+w(\boldsymbol{a}_{2k}\oplus\boldsymbol{a}_{2l})=8$$

证明：如果矩阵 $(\boldsymbol{A}_{i_1}^{\mathrm{T}},\boldsymbol{A}_{i_2}^{\mathrm{T}},\boldsymbol{A}_{i_3}^{\mathrm{T}})^{\mathrm{T}}$ 行置换同构于 $\begin{pmatrix}\boldsymbol{\alpha}_{j_0},\boldsymbol{\alpha}_{j_0},\bar{\boldsymbol{\alpha}}_{j_0},\bar{\boldsymbol{\alpha}}_{j_0}\\ \boldsymbol{\alpha}_{j_1},\bar{\boldsymbol{\alpha}}_{j_1},\boldsymbol{\alpha}_{j_1},\bar{\boldsymbol{\alpha}}_{j_1}\\ \boldsymbol{\alpha}_{j_2},\bar{\boldsymbol{\alpha}}_{j_2},\bar{\boldsymbol{\alpha}}_{j_2},\boldsymbol{\alpha}_{j_2}\end{pmatrix}$，那么 $\begin{cases}w(\boldsymbol{a}_{i_1k}\oplus\boldsymbol{a}_{i_1l})=4\\ w(\boldsymbol{a}_{i_2k}\oplus\boldsymbol{a}_{i_2l})=4\\ w(\boldsymbol{a}_{i_3k}\oplus\boldsymbol{a}_{i_3l})=0\end{cases}$，则有：

$$w(\boldsymbol{a}_{0k}\oplus\boldsymbol{a}_{0l})+w(\boldsymbol{a}_{1k}\oplus\boldsymbol{a}_{1l})+w(\boldsymbol{a}_{2k}\oplus\boldsymbol{a}_{2l})=8$$

3　分支数为 8 的 16 阶 0-1 可逆矩阵构造

由定义 1 可知，分支数为 8 的 16 阶 0-1 矩阵各行各列重量的最小值为 7，而 0-1 矩阵的重量越小，使用 0-1 矩阵的扩散结构实现速度就越快，占用资源就越少。因此，下文基于特征为 2 的域上 4 阶 0-1 矩阵和 4 阶 Hadmard 矩阵的结构和性质特点，给出一种各行各列重量都为 7 的分支数为 8 的 16 阶 0-1 可逆矩阵的结构和构造条件，并给予证明。

定理 2 矩阵 $\boldsymbol{A}_0$ 是各行各列重量都为 1 的 4 阶 0-1 矩阵，$\boldsymbol{A}_i=(\boldsymbol{a}_{i0},\boldsymbol{a}_{i1},\boldsymbol{a}_{i2},\boldsymbol{a}_{i3}),i=1,2,3$ 为各行各列重量都为 2 的行置换互不同构的 3 个 4 阶 0-1 矩阵，若满足以下 2 个条件：

(1) $(\boldsymbol{A}_{i_1}^{\mathrm{T}},\boldsymbol{A}_{i_2}^{\mathrm{T}},\boldsymbol{A}_{i_3}^{\mathrm{T}})^{\mathrm{T}}$ 行置换同构于 $\begin{pmatrix}\boldsymbol{\alpha}_{h_0},\boldsymbol{\alpha}_{h_0},\bar{\boldsymbol{\alpha}}_{h_0},\bar{\boldsymbol{\alpha}}_{h_0}\\ \boldsymbol{\alpha}_{h_1},\bar{\boldsymbol{\alpha}}_{h_1},\boldsymbol{\alpha}_{h_1},\bar{\boldsymbol{\alpha}}_{h_1}\\ \boldsymbol{\alpha}_{h_2},\bar{\boldsymbol{\alpha}}_{h_2},\bar{\boldsymbol{\alpha}}_{h_2},\boldsymbol{\alpha}_{h_2}\end{pmatrix}$，$1\leqslant i_1,i_2,i_3\leqslant 3$，$i_1,i_2,i_3$ 两两互不相等。

(2)当 $\boldsymbol{a}_{1j_1}\oplus\boldsymbol{a}_{2j_2}\oplus\boldsymbol{a}_{3j_3}=0$ 时，$\boldsymbol{a}_{0j_1}\oplus\boldsymbol{a}_{3j_2}\oplus\boldsymbol{a}_{2j_3}$、$\boldsymbol{a}_{3j_1}\oplus\boldsymbol{a}_{0j_2}\oplus\boldsymbol{a}_{1j_3}$、$\boldsymbol{a}_{2j_1}\oplus\boldsymbol{a}_{1j_2}\oplus\boldsymbol{a}_{0j_3}$ 这 3 个向量中至少有一个重量为 3，$0\leqslant j_1,j_2,j_3\leqslant 3$。

那么可逆矩阵 $\boldsymbol{A}=\begin{pmatrix}\boldsymbol{A}_0&\boldsymbol{A}_1&\boldsymbol{A}_2&\boldsymbol{A}_3\\ \boldsymbol{A}_1&\boldsymbol{A}_0&\boldsymbol{A}_3&\boldsymbol{A}_2\\ \boldsymbol{A}_2&\boldsymbol{A}_3&\boldsymbol{A}_0&\boldsymbol{A}_1\\ \boldsymbol{A}_3&\boldsymbol{A}_2&\boldsymbol{A}_1&\boldsymbol{A}_0\end{pmatrix}$ 是分支数为 8 的 16 阶 0-1 可逆矩阵。

证明：设 $\boldsymbol{Y}=\boldsymbol{A}\boldsymbol{X}$，$\boldsymbol{X}=(\boldsymbol{X}_0^{\mathrm{T}}\ \ \boldsymbol{X}_1^{\mathrm{T}}\ \ \boldsymbol{X}_2^{\mathrm{T}}\ \ \boldsymbol{X}_3^{\mathrm{T}})^{\mathrm{T}}$，$\boldsymbol{Y}=(\boldsymbol{Y}_0^{\mathrm{T}}\ \ \boldsymbol{Y}_1^{\mathrm{T}}\ \ \boldsymbol{Y}_2^{\mathrm{T}}\ \ \boldsymbol{Y}_3^{\mathrm{T}})^{\mathrm{T}}$，则：

$$\boldsymbol{Y}=\begin{pmatrix}\boldsymbol{Y}_0\\ \boldsymbol{Y}_1\\ \boldsymbol{Y}_2\\ \boldsymbol{Y}_3\end{pmatrix}=\boldsymbol{A}\boldsymbol{X}=\begin{pmatrix}\boldsymbol{A}_0&\boldsymbol{A}_1&\boldsymbol{A}_2&\boldsymbol{A}_3\\ \boldsymbol{A}_1&\boldsymbol{A}_0&\boldsymbol{A}_3&\boldsymbol{A}_2\\ \boldsymbol{A}_2&\boldsymbol{A}_3&\boldsymbol{A}_0&\boldsymbol{A}_1\\ \boldsymbol{A}_3&\boldsymbol{A}_2&\boldsymbol{A}_1&\boldsymbol{A}_0\end{pmatrix}\begin{pmatrix}\boldsymbol{X}_0\\ \boldsymbol{X}_1\\ \boldsymbol{X}_2\\ \boldsymbol{X}_3\end{pmatrix}$$

其中，$\boldsymbol{X},\boldsymbol{Y}$ 分别为特征为 2 的域上的 16 维 0-1 列向量，$\boldsymbol{X}_i,\boldsymbol{Y}_j$ 分别为 4 维 0-1 列向量，$i,j=0,1,2,3$。若记 $\boldsymbol{X}$ 的重量分布为 $w(\boldsymbol{X}_{g_0})-w(\boldsymbol{X}_{g_1})-w(\boldsymbol{X}_{g_2})-w(\boldsymbol{X}_{g_3}),0\leqslant g_0,g_1,g_2,g_3\leqslant 3$ $g_0,g_1,g_2,g_3\leqslant 3$，$g_0,g_1,g_2,g_3$ 两两互不相等，那么 $\boldsymbol{Y}$ 即为矩阵 $\boldsymbol{A}$ 的 $w(\boldsymbol{X})=w(\boldsymbol{X}_{g_0})+w(\boldsymbol{X}_{g_1})+w(\boldsymbol{X}_{g_2})+w(\boldsymbol{X}_{g_3})$ 列相加后得到的列向量，这 $w(\boldsymbol{X})$ 列为 4×4 的分块矩阵 $\boldsymbol{A}$ 中第 g_0 大列中的 $w(\boldsymbol{X}_{g_0})$ 列，第 g_1 大列中的 $w(\boldsymbol{X}_{g_1})$ 列，第 g_2 大列中的 $w(\boldsymbol{X}_{g_2})$ 列和第 g_3 大列中的 $w(\boldsymbol{X}_{g_3})$ 列。

根据定义 1 可知，要证明定理成立，即要证明当 $w(\boldsymbol{X})=1,2,\cdots,16$ 时不等式 $w(\boldsymbol{X})+w(\boldsymbol{Y})\geqslant 8$ 都成立。由于 $\boldsymbol{A}$ 是可逆矩阵，因此当 $w(\boldsymbol{X})=7,8,\cdots,16$ 时，显然 $w(\boldsymbol{X})+w(\boldsymbol{Y})\geqslant 8$ 成立。对于 $w(\boldsymbol{X})=1,2,\cdots,6$ 这 6 种情况，下面逐一讨论在这 6 种情况下不等式 $w(\boldsymbol{X})+w(\boldsymbol{Y})\geqslant 8$ 都成立。

当 $w(\boldsymbol{X})=1$，那么 $\boldsymbol{A}\boldsymbol{X}$ 即为矩阵 $\boldsymbol{A}$ 中的 1 列，根据条件知矩阵 $\boldsymbol{A}$ 中任意一列的重量都为 7，因此，$w(\boldsymbol{Y})=$

$w(\boldsymbol{AX})=7$，即在 $w(\boldsymbol{X})=1$ 这种情况下不等式 $w(\boldsymbol{X})+w(\boldsymbol{Y})\geqslant 8$ 显然成立。

当 $w(\boldsymbol{X})=2$，此时 $\boldsymbol{X}$ 的重量分布只能为 $2-0-0-0$ 和 $1-1-0-0$ 两种，因此，下面依次按这 2 种重量分布情况分别进行讨论：

情况 1 某个 $w(\boldsymbol{X}_p)=2$，则 $\boldsymbol{Y}=\boldsymbol{AX}$ 即为矩阵 $\boldsymbol{A}$ 的第 p 大列 $(\boldsymbol{A}_{p_0}{}^{\mathrm{T}},\boldsymbol{A}_{p_1}{}^{\mathrm{T}},\boldsymbol{A}_{p_2}{}^{\mathrm{T}},\boldsymbol{A}_{p_3}{}^{\mathrm{T}})^{\mathrm{T}}$ 的任意 2 列相加的结果。根据定理 1 知矩阵 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$ 中任意位置相同的 2 列中有一个矩阵的 2 列相同，另外 2 个矩阵的 2 列不同，由 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$ 的结构特点知 $\boldsymbol{A}_i$，$i=1,2,3$ 中互不相同的两列互补，而 $\boldsymbol{A}_0$ 中任意两列相加后的重量为 2，因此在 $w(\boldsymbol{X})=w(\boldsymbol{X}_p)=2$ 这种情况下，$w(\boldsymbol{Y})=w(\boldsymbol{AX})=4+4+2=10$，所以，这种情况下不等式 $w(\boldsymbol{X})+w(\boldsymbol{Y})\geqslant 8$ 成立。

情况 2 某 2 个 $w(\boldsymbol{X}_p)=w(\boldsymbol{X}_q)=1$，$p\neq q$，由 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$ 的结构特点知 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$ 中任意一个矩阵的一列与另外一个矩阵的一列相加后的重量为 2，$\boldsymbol{A}_0$ 中任意一列与 $\boldsymbol{A}_1$，$\boldsymbol{A}_2$，$\boldsymbol{A}_3$ 中任意一个矩阵的任意 1 列相加后的重量至少为 1，因此 $w(\boldsymbol{Y})\geqslant 2+2+1+1=6$，即在这种情况下不等式 $w(\boldsymbol{X})+w(\boldsymbol{Y})\geqslant 8$ 成立。

综合上述 2 种情况可知，当 $w(\boldsymbol{X})=2$ 时，不等式 $w(\boldsymbol{X})+w(\boldsymbol{Y})\geqslant 8$ 成立。

$w(\boldsymbol{X})=3,4,5,6$ 这 4 种情况的证明方法与 $w(\boldsymbol{X})=2$ 时的证明方法类似，都为分析性证明，因此，$w(\boldsymbol{X})=3,4,5,6$ 这 4 种情况可按 $w(\boldsymbol{X})=2$ 时的分析证明方法予以证明不等式 $w(\boldsymbol{X})+w(\boldsymbol{Y})\geqslant 8$ 仍然成立。

因此，满足定理条件的可逆矩阵：

$$\boldsymbol{A}=\begin{pmatrix}\boldsymbol{A}_0 & \boldsymbol{A}_1 & \boldsymbol{A}_2 & \boldsymbol{A}_3\\ \boldsymbol{A}_1 & \boldsymbol{A}_0 & \boldsymbol{A}_3 & \boldsymbol{A}_2\\ \boldsymbol{A}_2 & \boldsymbol{A}_3 & \boldsymbol{A}_0 & \boldsymbol{A}_1\\ \boldsymbol{A}_3 & \boldsymbol{A}_2 & \boldsymbol{A}_1 & \boldsymbol{A}_0\end{pmatrix}$$

为分支数为 8 的 16 阶 0-1 矩阵。证毕

显然，由定理 2 可以推出下面的结论。

推论 1 $\boldsymbol{A}_i=(\boldsymbol{a}_{i0},\boldsymbol{a}_{i1},\boldsymbol{a}_{i2},\boldsymbol{a}_{i3})$，$i=0,1,2,3$ 为 4 个 4 阶 0-1 矩阵，若其中一个矩阵为各行各列重量都为 1 的 4 阶 0-1 矩阵，另外 3 个为行置换互不同构的各行各列重量都为 2 的 4 阶 0-1 矩阵，若满足以下 2 个条件：

(1)3 个行置换互不同构的各行各列重量都为 2 的 4 阶 0-1 矩阵 $\boldsymbol{A}_{i_1},\boldsymbol{A}_{i_2},\boldsymbol{A}_{i_3}$ 构成的矩阵 $(\boldsymbol{A}_{i_1}{}^{\mathrm{T}},\boldsymbol{A}_{i_2}{}^{\mathrm{T}},\boldsymbol{A}_{i_3}{}^{\mathrm{T}})^{\mathrm{T}}$ 行置换同构于 $\begin{pmatrix}\boldsymbol{\alpha}_{h_0},\boldsymbol{\alpha}_{h_0},\bar{\boldsymbol{\alpha}}_{h_0},\bar{\boldsymbol{\alpha}}_{h_0}\\ \boldsymbol{\alpha}_{h_1},\bar{\boldsymbol{\alpha}}_{h_1},\boldsymbol{\alpha}_{h_1},\bar{\boldsymbol{\alpha}}_{h_1}\\ \boldsymbol{\alpha}_{h_2},\bar{\boldsymbol{\alpha}}_{h_2},\bar{\boldsymbol{\alpha}}_{h_2},\boldsymbol{\alpha}_{h_2}\end{pmatrix}$，$0\leqslant i_1,i_2,i_3\leqslant 3$，$i_1,i_2,i_3$ 两两互不相等。

(2)当 $\boldsymbol{a}_{i_1j_1}\oplus\boldsymbol{a}_{i_2j_2}\oplus\boldsymbol{a}_{i_3j_3}=0$ 时，$\boldsymbol{a}_{(i_1\oplus 1)j_1}\oplus\boldsymbol{a}_{(i_2\oplus 1)j_2}\oplus\boldsymbol{a}_{(i_3\oplus 1)j_3}$，$\boldsymbol{a}_{(i_1\oplus 2)j_1}\oplus\boldsymbol{a}_{(i_2\oplus 2)j_2}\oplus\boldsymbol{a}_{(i_3\oplus 2)j_3}$，$\boldsymbol{a}_{(i_1\oplus 3)j_1}\oplus\boldsymbol{a}_{(i_2\oplus 3)j_2}\oplus\boldsymbol{a}_{(i_3\oplus 3)j_3}$ 这 3 个向量中至少有一个重量为 3，$0\leqslant j_1,j_2,j_3\leqslant 3$。

那么可逆矩阵：

$$\boldsymbol{A}=\begin{pmatrix}\boldsymbol{A}_0 & \boldsymbol{A}_1 & \boldsymbol{A}_2 & \boldsymbol{A}_3\\ \boldsymbol{A}_1 & \boldsymbol{A}_0 & \boldsymbol{A}_3 & \boldsymbol{A}_2\\ \boldsymbol{A}_2 & \boldsymbol{A}_3 & \boldsymbol{A}_0 & \boldsymbol{A}_1\\ \boldsymbol{A}_3 & \boldsymbol{A}_2 & \boldsymbol{A}_1 & \boldsymbol{A}_0\end{pmatrix}$$

是分支数为 8 的 16 阶 0-1 可逆矩阵。

推论 1 给出了较定理 2 更为一般的关于分支数为 8 的 16 阶 0-1 可逆矩阵的结构和满足的条件，再利用行、列置换的方法，结合引理 1 即可根据推论 1 构造大量分支数为 8 的 16 阶 0-1 可逆矩阵。

4 16 阶 Hadamard 型对合 0-1 可逆矩阵的构造

基于推论 1，结合定义 3 和引理 2，对于对合 0-1 矩阵有如下结论：

推论 2 $\boldsymbol{A}_i=(\boldsymbol{a}_{i0},\boldsymbol{a}_{i1},\boldsymbol{a}_{i2},\boldsymbol{a}_{i3})$，$i=0,1,2,3$ 为 4 个 4 阶 Hadamard 型 0-1 矩阵，若其中一个矩阵为各行各列重量都为 1 的 4 阶 0-1 矩阵，另外 3 个为行置换互不同构的各行各列重量都为 2 的 4 阶 0-1 矩阵，那么矩阵：

$$\boldsymbol{A}=\begin{pmatrix}\boldsymbol{A}_0 & \boldsymbol{A}_1 & \boldsymbol{A}_2 & \boldsymbol{A}_3\\ \boldsymbol{A}_1 & \boldsymbol{A}_0 & \boldsymbol{A}_3 & \boldsymbol{A}_2\\ \boldsymbol{A}_2 & \boldsymbol{A}_3 & \boldsymbol{A}_0 & \boldsymbol{A}_1\\ \boldsymbol{A}_3 & \boldsymbol{A}_2 & \boldsymbol{A}_1 & \boldsymbol{A}_0\end{pmatrix}$$

是分支数为 8 的 16 阶对合 0-1 矩阵，并且这样的矩阵 $\boldsymbol{A}$ 有 $8\times 4!$ 类。

证明：首先证明矩阵 $\boldsymbol{A}$ 是分支数为 8 的 16 阶对合 0-1 矩阵。

由 Hadamard 矩阵的结构特点知：若 $\boldsymbol{A}_0$，$\boldsymbol{A}_1$，$\boldsymbol{A}_2$，$\boldsymbol{A}_3$ 为 Hadamard 型 0-1 矩阵，则矩阵 $\boldsymbol{A}$ 为 Hadamard 型 0-1 矩阵。本文构造的 $\boldsymbol{A}$ 是各行各列重量都为 7 的矩阵，因此，根据引理 2 知 $\boldsymbol{A}\cdot\boldsymbol{A}=\boldsymbol{E}$，即矩阵 $\boldsymbol{A}$ 是对合矩阵，显然对合 0-1 矩阵一定是可逆矩阵。

记：

$\boldsymbol{e}_0=(1\ \ 0\ \ 0\ \ 0)^{\mathrm{T}}$，$\boldsymbol{e}_1=(0\ \ 1\ \ 0\ \ 0)^{\mathrm{T}}$

$\boldsymbol{e}_2=(0\ \ 0\ \ 1\ \ 0)^{\mathrm{T}}$，$\boldsymbol{e}_3=(0\ \ 0\ \ 0\ \ 1)^{\mathrm{T}}$

各行各列重量都为 1 的 4 阶 Hadamard 型 0-1 矩阵共有 4 个，分别为：

$(\boldsymbol{e}_0\ \ \boldsymbol{e}_1\ \ \boldsymbol{e}_2\ \ \boldsymbol{e}_3)$，$(\boldsymbol{e}_1\ \ \boldsymbol{e}_0\ \ \boldsymbol{e}_3\ \ \boldsymbol{e}_2)$

$(\boldsymbol{e}_2\ \ \boldsymbol{e}_3\ \ \boldsymbol{e}_0\ \ \boldsymbol{e}_1)$，$(\boldsymbol{e}_3\ \ \boldsymbol{e}_2\ \ \boldsymbol{e}_1\ \ \boldsymbol{e}_0)$

各行各列重量都为 2 的 4 阶 Hadamard 型 0-1 矩阵共有 6 个，分别为：

$(\boldsymbol{\alpha}_0,\boldsymbol{\alpha}_0,\bar{\boldsymbol{\alpha}}_0,\bar{\boldsymbol{\alpha}}_0)$，$(\bar{\boldsymbol{\alpha}}_0,\bar{\boldsymbol{\alpha}}_0,\boldsymbol{\alpha}_0,\boldsymbol{\alpha}_0)$，$(\boldsymbol{\alpha}_1,\bar{\boldsymbol{\alpha}}_1,\bar{\boldsymbol{\alpha}}_1,\boldsymbol{\alpha}_1)$

$(\bar{\boldsymbol{\alpha}}_1,\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_1,\bar{\boldsymbol{\alpha}}_1)$，$(\boldsymbol{\alpha}_2,\bar{\boldsymbol{\alpha}}_2,\boldsymbol{\alpha}_2,\bar{\boldsymbol{\alpha}}_2)$，$(\bar{\boldsymbol{\alpha}}_2,\boldsymbol{\alpha}_2,\bar{\boldsymbol{\alpha}}_2,\boldsymbol{\alpha}_2)$

而这 6 个矩阵中任意 3 个行置换互不同构的矩阵都满足推论 1 的条件(1)，且这样的 3 元组总共有 8 个。经检测

上面 4 个 4 阶 Hadamard 型 0-1 矩阵对于这样 3 个行置换互不同构的矩阵都满足推论 1 的条件(2)，那么由推论 1 知构造的矩阵 $\boldsymbol{A}$ 是分支数为 8 的 16 阶对合 0-1 矩阵。

由上面的证明过程知满足推论 1 条件的各行各列重量都为 1 的 4 阶 Hadamard 型 0-1 矩阵共有 4 个，分别为：

$(\boldsymbol{e}_0 \quad \boldsymbol{e}_1 \quad \boldsymbol{e}_2 \quad \boldsymbol{e}_3), (\boldsymbol{e}_1 \quad \boldsymbol{e}_0 \quad \boldsymbol{e}_3 \quad \boldsymbol{e}_2)$

$(\boldsymbol{e}_2 \quad \boldsymbol{e}_3 \quad \boldsymbol{e}_0 \quad \boldsymbol{e}_1), (\boldsymbol{e}_3 \quad \boldsymbol{e}_2 \quad \boldsymbol{e}_1 \quad \boldsymbol{e}_0)$

显然，这 4 个矩阵中任意 1 个矩阵分别在行置换 (1 0 3 2)、(2 3 0 1)、(3 2 1 0) 的作用下与另外 3 个矩阵是分别相同的。而满足推论 1 的条件(1)的 4 阶 Hadamard 型 0-1 矩阵 $\boldsymbol{A}_{i_1}$、$\boldsymbol{A}_{i_2}$、$\boldsymbol{A}_{i_3}$ 分别同时在行置换 (1 0 3 2)或(2 3 0 1) 或(3 2 1 0) 的作用后仍满足推论 1 的条件(1)。因此，对任意一组满足推论 1 条件的 Hadamard 型 0-1 矩阵 $\boldsymbol{A}_0$、$\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$，这组矩阵分别在行置换 (1 0 3 2) 或 (2 3 0 1) 或 (3 2 1 0) 的作用后仍然满足推论 1 的条件，由 Hadamard 矩阵的结构特点可知，矩阵 $\boldsymbol{A}$ 由 $\boldsymbol{A}_0$、$\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$ 完全确定，因此，该方法构造出的不同的 0-1 矩阵中任意一个矩阵都与另外 3 个矩阵行置换同构，显然该方法可构造出行置换互不同构的 0-1 矩阵共 $4\times 8\times 4!/4 = 8\times 4!$ 类。证毕。

由推论 2 构造出的 16 阶 0-1 矩阵的结构特点知，若对推论 2 构造出的 0-1 矩阵进行行、列置换后的矩阵仍为对称矩阵，则置换后的 0-1 矩阵仍然为对合矩阵。因此，利用推论 2 构造 0-1 矩阵的方法和矩阵行、列置换的方法可以构造出大量的分支数为 8 的 16 阶 0-1 对合矩阵。例如选：

$$\boldsymbol{A}_0 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \boldsymbol{A}_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\boldsymbol{A}_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \boldsymbol{A}_3 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

则矩阵：

$$\boldsymbol{A} = \begin{pmatrix} \boldsymbol{A}_0 & \boldsymbol{A}_1 & \boldsymbol{A}_2 & \boldsymbol{A}_3 \\ \boldsymbol{A}_1 & \boldsymbol{A}_0 & \boldsymbol{A}_3 & \boldsymbol{A}_2 \\ \boldsymbol{A}_2 & \boldsymbol{A}_3 & \boldsymbol{A}_0 & \boldsymbol{A}_1 \\ \boldsymbol{A}_3 & \boldsymbol{A}_2 & \boldsymbol{A}_1 & \boldsymbol{A}_0 \end{pmatrix}$$

即为一个分支数为 8 的 16 阶对合 0-1 矩阵，发现 ARIA 算法扩散结构所使用的 0-1 对合矩阵即为该矩阵经过行置换 (0 1 2 3 6 7 4 5 9 8 11 10 15 14 13 12) 后得到的矩阵。

5 结束语

根据特征为 2 的域上 4 阶 0-1 矩阵和 Hadamard 矩阵的结构和性质特点，本文利用分块构造矩阵给出构造一类具有最大分支数的 16 阶 0-1 矩阵的方法。利用该方法构造的矩阵，各行各列重量均达到了具有最大分支数的 16 阶 0-1 矩阵行列重量的最小值 7，具有实现速度快、占用资源少的特点。下一步将研究更为一般性的具有最大分支数的 0-1 矩阵构造方法。

参考文献

[1] Daemen J, Rijmen V. The Wide Trail Design Strategy[EB/OL]. (2001-03-12). http://130.203.133.150/viewdoc/summary?doi=10.1.1.85.2588.

[2] Wang Meiqin. Differential Cryptanalysis of Present[EB/OL]. (2007-10-14). http://eprint.iacr.org/2007/408.

[3] Rijmen V, Daemen J, Preneel B, et al. The Cipher Shark[EB/OL]. (1996-04-20). http://link.springer.com/chapter/10.1007%2F3-540-60865-6_47.

[4] Kang Ju-sung, Hong Seokhie, Lee Sangjin, et al. Practical and Provable Security Against Differential and Linear Cryptanalysis for Substitution-permutation Networks[J]. ETRI Journal, 2001, 23(4): 158-167.

[5] Aoki K, Ichikawa T, Kanda M, et al. Camellia: A 128-bit Block Cipher Suitable for Multiple Platforms-design and Analysis[EB/OL]. (2000-04-09). http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.25.9586.

[6] NTT-Nippon Telegraph and Telephone Corporation. E2: Efficient Encryption Algorithm[EB/OL]. (2007-02-02). http://info.isl.ntt.co.jp/e2.

[7] Kwon D, Kim J, Park S, et al. New Block Cipher: ARIA[EB/OL]. (2004-05-10). http://link.springer.com/chapter/10.1007%2F978-3-540-24691-6_32?LI=true.

[8] 吴文玲, 冯登国, 张文涛. 分组密码的设计与分析[M]. 2 版. 北京: 清华大学出版社, 2009.

[9] Gao Ying, Guo Guifeng. Unified Approach to Construct 8×8 Matrices with Branch Number 5[C]//Proc. of CDEE'10. Qinhuangdao, China: [s. n.], 2010.

[10] 崔 霆, 陈河山, 金晨辉. 分组密码二元扩散结构的几点注记[J]. 软件学报, 2012, 23(9): 2430-2437.

[11] Aslan B, Sakall M T. Algebraic Construction of Cryptographically Good Binary Linear Transformations[EB/OL]. (2012-05-09). http://onlinelibrary.wiley.com/doi/10.1002/sec.556/abstract.

[12] Lu Xiao, Heys H. Hardware Design and Analysis of Block Cipher Components[EB/OL]. (2002-12-04). http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.14.2543.

编辑 金胡考