一类 ARIA 型扩散结构分支数的研究

马宿东,金晨辉,关 杰
(战略支援部队信息工程大学,河南郑州 450001)

摘 要: 分支数达到最大的二元矩阵被广泛应用到分组密码扩散层的设计中. 本文针对 ARIA 算法的扩散层,首先给出了 ARIA 型扩散结构的定义,给出了 16 阶 ARIA 型扩散结构的分支数情况,进一步给出了分支数为 8 的 16 阶 ARIA 型扩散结构的充要条件,从而构造了一大批可供选择的分支数为 8 的 16 阶二元矩阵. 其次,解决了 16 阶 ARIA 型扩散结构分支数为 8 的计数问题,最后,给出了分支数为 8 的 16 阶对合 ARIA 型扩散结构的构造方法. 本文的研究成果为构造分支数达到最大的 16 阶对合二元方阵提供了一种新方法.

关键词: 分组密码; ARIA 算法; 扩散结构; 二元矩阵; 分支数; ARIA 型扩散结构; 对合矩阵
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2020)03-0449-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.03.005

Research on the Branch Number of ARIA-Type Diffusion Structures

MA Su-dong, JIN Chen-hui, GUAN Jie
(*Strategic Support Force Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: The binary matrix with the largest branch number is widely used in the design of diffusion layers in block cipher. In this paper, for the diffusion layer of ARIA algorithm, the definition of ARIA diffusion structure is given firstly, and the branch number of 16-order ARIA diffusion structure is given. The necessary and sufficient conditions for the 16-order ARIA-type diffusion structures with the branch number 8 are further given, and a large number of 16-order ARIA-type diffusion structures with the branch number 8 are constructed. Secondly, the counting problem of 16-order ARIA-type diffusion structures with the branch number 8 is solved. Finally, the construction methods of the 16-order involution ARIA-type diffusion structure are given. The research results of this paper provide a method for constructing 16-order involution binary matrix with the largest branch number.

Key words: block cipher; ARIA algorithm; diffusion layer; binary matrix; branch number; ARIA-type diffusion structures; involution matrix

1 引言

线性扩散层是分组密码的重要部件之一,而分支数是刻画其设计好坏的重要指标,具有较大的分支数可以更有效地抵抗差分和线性密码分析. 对于一个 n 级 GF(2^m) 上的矩阵,其分支数最大可以达到 $n+1$,分支数达到最大的矩阵称为 MDS 矩阵.

虽然可以利用 GF(2^m) 上的矩阵设计出分支数达到最大的扩散层,但是 GF(2^m) 上的矩阵通常需要处理有限域上的乘法[1]. 如果使用 GF(2^m) 上的二元矩阵设计扩散层,虽然分支数不能达到最大值,但是非常利于软、硬件实现并且占用资源少. 因此,二元矩阵在分组密码的扩散层设计中得到广泛应用,例如 E2[2]、Camellia[3]、ARIA[4] 等算法均采用了 8 阶或 16 阶二元矩阵设计扩散层,而 8 阶和 16 阶二元矩阵最大分支数分别为 5[5] 和 8[6],32 阶二元矩阵分支数最大值被认为是 12[7],尚未得到证明. 因此,如何构造分支数达到最大值的二元矩阵成为分组密码研究的热点问题.

文献[8]针对一类特殊形式的矩阵,给出了一种构造分支数为 5 的 8 阶二元矩阵的方法. 文献[9]利用矩阵分块的思想,给出了一类分支数为 8 且行重量和列重量都为 7 的 16 阶二元矩阵的构造方法. 文献[10]提出了一种新的代数构造方法生成了分支数为 12 的 32 阶二元方阵. 文献[11]提出了一种新的方法构造分支数

收稿日期:2019-02-21;修回日期:2019-06-08;责任编辑:覃怀银
基金项目:国家自然科学基金(No. 61572516, No. 61272041, No. 61272488)

达到最大值的 $k\cdot 2^t$ 阶二元方阵. 文献[12]提出了分而治之的方法构造分支数达到最大且每行每列具有相同汉明重量的 n 阶二元矩阵.

在文献[13]中,作者设计了一个分支数为 8 的 16 阶二元对合矩阵,随后被用作韩国分组密码标准 ARIA 算法的扩散层. 该扩散层是由三层扩散结构 $\boldsymbol{A}=\boldsymbol{MHM}$ 构成,是以小规模扩散层 $\boldsymbol{M},\boldsymbol{H}$ 为基础,通过简单的复合来构造大规模扩散层. 其优点是在各种平台上适应性好,硬件实现易于控制,实现代价较低. 然而,对于这种复合型扩散结构,文献[13]只构造了一个分支数为 8 的 16 阶二元矩阵,还有一些问题没有解决,比如能否利用该复合结构构造其它分支数为 8 的 16 阶二元矩阵以及能否构造分支数为 8 的 16 阶对合型二元矩阵,尚没有理论上的结论.

针对上述问题,本文首先给出了 ARIA 型扩散结构的定义,证明了 16 阶 ARIA 型扩散结构的分支数只能为 4 或者 8,并给出了分支数为 8 的 16 阶 ARIA 型扩散结构的充要条件;其次,解决了 16 阶 ARIA 型扩散结构分支数为 8 的计数问题;最后,给出了分支数为 8 的 16 阶对合 ARIA 型扩散结构的构造方法,通过该方法,可以构造 9312 个不同的分支数为 8 的 16 阶对合二元矩阵.

2 ARIA 型扩散结构

文献[14]针对 $\mathrm{GF}(2^m)$ 上的线性变换,证明了以下结论:

命题 1[14] 设 $f(x)=\boldsymbol{A}\boldsymbol{x}$ 且 $\boldsymbol{A}$ 是 $\mathrm{GF}(2^m)$ 上的 $n\times n$ 矩阵,对于 $\mathrm{GF}(2^m)$ 上的 n 维向量 $\boldsymbol{x}$,记 $W(\boldsymbol{x})$ 是 $\boldsymbol{x}$ 的非零分量的个数,则有

(1)f 的差分分支数和线性分支数分别满足

$$D_f^{(m)}=\min\{W(\boldsymbol{x})+W(\boldsymbol{A}\boldsymbol{x}):\boldsymbol{x}\in[\mathrm{GF}(2^m)^n]\setminus\{0\}\}$$

和

$$L_f^{(m)}=\min\{W(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{x})+W(\boldsymbol{x}):\boldsymbol{x}\in[\mathrm{GF}(2^m)^n]\setminus\{0\}\};$$

(2)如果 $\boldsymbol{A}$ 是 $\mathrm{GF}(2^m)$ 上的正交矩阵,即 $\boldsymbol{A}^{-1}=\boldsymbol{A}^{\mathrm{T}}$,则 f 的差分分支数和线性分支数相等.

定义 1 如果矩阵 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 同时满足

(1)$\boldsymbol{M}_1,\boldsymbol{M}_2$ 为每行每列都仅有一个 $\mathrm{GF}(2^m)$ 上的 4 级全 0 矩阵、其它位置都是 $\mathrm{GF}(2^m)$ 上的 4 级单位矩阵的 $n\times n$ 分块矩阵;

(2)$\boldsymbol{H}=\mathrm{diag}(\boldsymbol{H}_1,\cdots,\boldsymbol{H}_n)$,这里 $\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_n$ 为 $\mathrm{GF}(2^m)$ 上每行每列仅有一个 0 的 4×4 矩阵.

则称 $\boldsymbol{A}$ 为 $\mathrm{GF}(2^m)$ 上的 ARIA 型扩散结构,并分别称 $\boldsymbol{M}_1,\boldsymbol{M}_2$ 为 ARIA 型扩散结构的第一层和第三层,称 $\boldsymbol{H}$ 为 ARIA 型扩散结构的中间层.

图 1 为 ARIA 型扩散结构的结构框图.

在定义 1 中,取 $n=4,m=8$,令

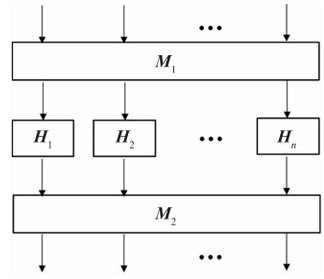

图1 ARIA型扩散结构

$$\boldsymbol{M}_1=\boldsymbol{M}_2=\boldsymbol{M}=\begin{bmatrix}E&E&E&0\\E&0&E&E\\E&E&0&E\\0&E&E&E\end{bmatrix}$$

令

$$\boldsymbol{H}_1=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{bmatrix},\boldsymbol{H}_2=\begin{bmatrix}1&0&1&1\\0&1&1&1\\1&1&1&0\\1&1&0&1\end{bmatrix},$$

$$\boldsymbol{H}_3=\begin{bmatrix}1&1&0&1\\1&1&1&0\\0&1&1&1\\1&0&1&1\end{bmatrix},\boldsymbol{H}_4=\begin{bmatrix}1&1&1&0\\1&1&0&1\\1&0&1&1\\0&1&1&1\end{bmatrix},$$

则此时的扩散结构 $\boldsymbol{A}=\boldsymbol{MHM}$ 就是 ARIA 算法的扩散层[4].

引理 1 设 $\mathrm{GF}(2^m)$ 上的方阵 $\boldsymbol{B}$ 是块数 n 为偶数的分块方阵,且各分块矩阵只取 k 级全 0 方阵和 k 级单位方阵,如果 $\boldsymbol{B}$ 的每行每列仅有一个全 0 方阵,则 $\boldsymbol{B}$ 为正交矩阵.

证明 设分块矩阵 $\boldsymbol{B}$ 的第 i 行的第 $p(i)$ 列位置为全 0 方阵,则 p 为 $\{1,2,\cdots,n\}$ 到自身的双射. 再设矩阵 $\boldsymbol{P}$ 是仅在 $i\times p(i)$ 位置为 k 级单位方阵、其它位置都是 k 级全 0 方阵的分块矩阵,则有 $\boldsymbol{B}=\boldsymbol{I}\oplus\boldsymbol{P}$,这里分块矩阵 I 的元素全是单位矩阵. 则由分块矩阵 $\boldsymbol{B}$ 的级数是偶数知

$$\begin{aligned}\boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}&=(\boldsymbol{I}\oplus\boldsymbol{P})(\boldsymbol{I}\oplus\boldsymbol{P})^{\mathrm{T}}=(\boldsymbol{I}\oplus\boldsymbol{P})(\boldsymbol{I}\oplus\boldsymbol{P}^{\mathrm{T}})\\&=\boldsymbol{I}\times\boldsymbol{I}\oplus\boldsymbol{I}\times\boldsymbol{P}^{\mathrm{T}}\oplus\boldsymbol{P}\times\boldsymbol{I}\oplus\boldsymbol{P}\boldsymbol{P}^{\mathrm{T}}=\boldsymbol{P}\boldsymbol{P}^{\mathrm{T}}=\boldsymbol{E}.\end{aligned}$$

证毕

定义 1 的 $\boldsymbol{M}$ 和 $\boldsymbol{H}_i$ 就是引理 1 中 $k=4$ 或 1 时的矩阵 $\boldsymbol{B}$.

如果矩阵 $\boldsymbol{B}$ 的逆就是 $\boldsymbol{B}$,则称 $\boldsymbol{B}$ 是对合矩阵. 由正交矩阵和对合矩阵的定义即可证明定理 1.

定理 1 (1)$\mathrm{GF}(2^m)$ 上的 ARIA 型扩散结构 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 是正交矩阵;

(2)若 $\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_n$ 均是对合矩阵且 $\boldsymbol{M}_1=\boldsymbol{M}_2^{-1}$,则 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 是对合矩阵.

再由命题 1 的(2)可得以下推论.

推论　ARIA 型扩散结构的差分分支数与线性分支数相等.

据此,以下不再区分 ARIA 型扩散结构的差分分支数和线性分支数,而将之简称为分支数.

3　ARIA 型扩散结构的性质

定义 2　设 $x_1,x_2,\cdots,x_n\in \mathrm{GF}(2^m)$,如果存在$\{1,2,\cdots,n\}$到自身的双射 p,使得

$$f_p(x_1,x_2,\cdots,x_n)=(x_{p(1)},x_{p(2)},\cdots,x_{p(n)})$$

则称 f_p 是由 p 定义的块移位变换. 再设 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)^{\mathrm{T}}$,且由 p 定义的块移位变换 $f_p(\boldsymbol{x})=\boldsymbol{P}\boldsymbol{x}$,则称矩阵 $\boldsymbol{P}$ 为由 p 定义的置换矩阵,此时矩阵 $\boldsymbol{P}$ 是第 i 行仅在第 $p(i)$ 列为 1 的二元方阵.

由分支数的定义易证引理 2.

引理 2　(1)4 级二元方阵 $\boldsymbol{A}$ 的分支数为 4 的充要条件是每行每列仅有 1 个 0;

(2)分支数为 4 的 4 级二元方阵的个数为 24.

设 $\mathrm{GF}(2^m)$ 上的 4×4 方阵 $\boldsymbol{H}$ 是各行各列仅有 1 个位置为 0 的二元矩阵,记第 i 行为 0 的列是 $p(i)$,记 $\boldsymbol{P}$ 是 $\mathrm{GF}(2^m)$ 上由 p 定义的置换矩阵,则有 $\boldsymbol{H}=\boldsymbol{I}\oplus\boldsymbol{P}$. 显然,这些方阵 $\boldsymbol{H}$ 与$\{1,2,3,4\}$到自身的双射一一对应.

命题 2　设 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$ 都是 $\mathrm{GF}(2^m)$ 上各行各列仅有 1 个 0 的 n 级二元方阵,$f_1(\boldsymbol{x})=\boldsymbol{H}_1\boldsymbol{x}$,$f_2(\boldsymbol{x})=\boldsymbol{H}_2\boldsymbol{x}$,则分别存在$[\mathrm{GF}(2^m)]^n\to[\mathrm{GF}(2^m)]^n$ 的块移位变换 f_{s_1},f_{s_2},使得

$$f_2(\boldsymbol{x})=f_1(f_{s_1}(\boldsymbol{x})),f_2(\boldsymbol{x})=f_{s_2}(f_1(\boldsymbol{x})).$$

证明　这里只证存在 f_{s_1},使得 $f_2(\boldsymbol{x})=f_1(f_{s_1}(\boldsymbol{x}))$ 成立,另一半结论同理可证.

设 $\boldsymbol{I}$ 是全 1 方阵,则 $\boldsymbol{H}_1\boldsymbol{x}=(\boldsymbol{I}\oplus\boldsymbol{P}_1)\boldsymbol{x}$. 再设 $f_I(\boldsymbol{x})=\boldsymbol{I}\boldsymbol{x}$,$f_{P_1}(\boldsymbol{x})=\boldsymbol{P}_1\boldsymbol{x}$,再设 $\boldsymbol{S}$ 是由 s 定义的置换矩阵,$f_S(\boldsymbol{x})=\boldsymbol{S}\boldsymbol{x}$ 是对应的块移位变换,则有

$$\begin{aligned}f_1(f_s(\boldsymbol{x}))&=\boldsymbol{H}_1\boldsymbol{S}\boldsymbol{x}=\boldsymbol{I}\boldsymbol{S}\boldsymbol{x}\oplus\boldsymbol{P}_1\boldsymbol{S}\boldsymbol{x}\\&=\boldsymbol{I}\boldsymbol{x}\oplus\boldsymbol{P}_1\boldsymbol{S}\boldsymbol{x}=(\boldsymbol{I}\oplus\boldsymbol{P}_1\boldsymbol{S})\boldsymbol{x},\end{aligned}$$

由于 $\boldsymbol{P}_1\boldsymbol{S}$ 是由 $p(s(i))$ 定义的置换矩阵,定义块移位变换 q,使得 $q(i)=p(s(i))$,则有 $f_1(f_s(\boldsymbol{x}))=f_2(\boldsymbol{x})$.

证毕

命题 2 描述的是,对任意分支数为 4 的二元方阵的输入或者输出施加一个块移位变换,可得所有分支数为 4 的二元方阵.

引理 3[14]　设 P 是 $\mathrm{GF}(2^m)$ 上具有 n 个输入变量和 n 个输出变量的线性变换,p 和 q 都是$\{1,2,\cdots,n\}$到自身的双射,f_p和f_q分别为由 p 和 q 定义的块移位变换,定义 $\mathrm{GF}(2^m)$ 上的线性变换 $f(\boldsymbol{x})=f_q(P(f_p(\boldsymbol{x})))$,则 f 的差分分支数等于 P 的差分分支数,f 的线性分支数等于 P 的线性分支数.

由引理 3 及定义 2 即得定理 2.

定理 2　对于给定的 $\boldsymbol{H}$,只要 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$ 的选择满足定义 1 之(1),ARIA 型扩散结构 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 的分支数就都相等.

下面证明:交换中间层 $\boldsymbol{H}_1,\boldsymbol{H}_2,\cdots,\boldsymbol{H}_n$ 的位置,也不改变 ARIA 型扩散结构的分支数.

定理 3　设线性变换 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 为 ARIA 型扩散结构,再设 p 是$\{1,2,\cdots,n\}$到自身的双射,线性变换 $\boldsymbol{H}_f=\mathrm{diag}(\boldsymbol{H}_{p(1)},\boldsymbol{H}_{p(2)},\cdots,\boldsymbol{H}_{p(n)})$,则扩散结构 $\boldsymbol{B}=\boldsymbol{M}_2\cdot\boldsymbol{H}_f\cdot\boldsymbol{M}_1$ 的分支数与 $\boldsymbol{A}$ 相同.

证明　设$(y_1,y_2,\cdots,y_n)^{\mathrm{T}}=\boldsymbol{H}_f\cdot(x_1,x_2,\cdots,x_n)^{\mathrm{T}}$,则对 $1\leqslant i\leqslant n$,有 $y_i=\boldsymbol{H}_{p(i)}x_i$,故 $y_{p^{-1}(i)}=\boldsymbol{H}_ix_{p^{-1}(i)}$,因而有 $f_{p^{-1}}\boldsymbol{y}=\boldsymbol{H}f_{p^{-1}}\boldsymbol{x}$,这里 $f_{p^{-1}}$为由 p^{-1}定义的块移位变换. 由此可得 $\boldsymbol{y}=f_p\boldsymbol{H}f_{p^{-1}}\boldsymbol{x}$,故 $\boldsymbol{H}_f=f_p\boldsymbol{H}f_{p^{-1}}$. 从而有 $\boldsymbol{B}=\boldsymbol{M}_2f_p\boldsymbol{H}f_{p^{-1}}\boldsymbol{M}_1$. 由命题 2 可知,存在由矩阵 $\boldsymbol{\theta}_1,\boldsymbol{\theta}_2$ 定义的块移位变换 $f_{\theta_1},f_{\theta_2}$,使得

$f_{p^{-1}}\boldsymbol{M}_1=\boldsymbol{M}_1f_{\theta_1}$和 $\boldsymbol{M}_2f_p=f_{\theta_2}\boldsymbol{M}_2$ 成立.

因此,可得 $\boldsymbol{B}=f_{\theta_2}\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1f_{\theta_1}$. 由定理 2 可知 $\boldsymbol{B}$ 的分支数与 $\boldsymbol{A}$ 相同.

证毕

类似定理 3 的证明可证定理 4. 再由命题 2 可知,ARIA 型复合结构的分支数与中间层第一个小块矩阵的选取无关.

定理 4　设线性变换 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 是 ARIA 型复合结构,再设 θ,λ 分别为由 p,q 定义的块移位变换,线性变换 $\boldsymbol{\lambda}\boldsymbol{H}\boldsymbol{\theta}=(\boldsymbol{\lambda}\boldsymbol{H}_1\boldsymbol{\theta},\boldsymbol{\lambda}\boldsymbol{H}_2\boldsymbol{\theta},\boldsymbol{\lambda}\boldsymbol{H}_3\boldsymbol{\theta},\boldsymbol{\lambda}\boldsymbol{H}_4\boldsymbol{\theta})$,则复合结构 $\boldsymbol{B}=\boldsymbol{M}_2\cdot\boldsymbol{\lambda}\boldsymbol{H}\boldsymbol{\theta}\cdot\boldsymbol{M}_1$ 的分支数与 $\boldsymbol{A}$ 相同.

4　一类 16 阶 ARIA 型扩散结构

当 $n=4$ 时,称定义 1 中的 ARIA 型扩散结构为 $\mathrm{GF}(2^m)$ 上的 16 阶 ARIA 型扩散结构.

引理 4　设 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 为 $\mathrm{GF}(2^m)$ 上的 16 阶 ARIA 型扩散结构,则对任意非零的 $\boldsymbol{x}$,都有

$$W(\boldsymbol{x})+W(\boldsymbol{A}\boldsymbol{x})\geqslant4.$$

证明　(1)设 $W(\boldsymbol{x})=1$ 且 $\boldsymbol{x}$ 的非零分量的值是 a. 则 $\boldsymbol{H}_1,\boldsymbol{H}_2,\boldsymbol{H}_3,\boldsymbol{H}_4$ 中有 1 个的输入是全 0 的 4 维向量,另外 3 个的输入是重量为 1 的 4 维向量且其非零的分量都是 a,因此,$\boldsymbol{H}_1,\boldsymbol{H}_2,\boldsymbol{H}_3,\boldsymbol{H}_4$ 中有 1 个的输出是全 0 的 4 维向量,另外 3 个的输出是重量为 3 的 4 维向量且其非零的分量都是 a. 不妨设这 3 个重量为 3 的 4 维向量为

$$\boldsymbol{b}_1=\boldsymbol{I}_a\oplus\boldsymbol{e}_1,\boldsymbol{b}_2=\boldsymbol{I}_a\oplus\boldsymbol{e}_2,\boldsymbol{b}_3=\boldsymbol{I}_a\oplus\boldsymbol{e}_3,$$

这里 $\boldsymbol{I}_a$ 是分量全为 a 的 4 维向量,则在 $\boldsymbol{M}_2$的 4 个输出块中,有 1 个输出块是

$$\boldsymbol{b}_1\oplus\boldsymbol{b}_2\oplus\boldsymbol{b}_3=\boldsymbol{I}_a\oplus\boldsymbol{e}_1\oplus\boldsymbol{e}_2\oplus\boldsymbol{e}_3,$$

其它3个输出块为

$\boldsymbol{b}_1\oplus\boldsymbol{b}_2=\boldsymbol{e}_1\oplus\boldsymbol{e}_2,\boldsymbol{b}_2\oplus\boldsymbol{b}_3=\boldsymbol{e}_2\oplus\boldsymbol{e}_3,\boldsymbol{b}_3\oplus\boldsymbol{b}_1=\boldsymbol{e}_3\oplus\boldsymbol{e}_1$.

如果 $\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3$ 至少有两个相等,则 $\boldsymbol{e}_1\oplus\boldsymbol{e}_2\oplus\boldsymbol{e}_3$ 的重量是1,因而 $\boldsymbol{b}_1\oplus\boldsymbol{b}_2\oplus\boldsymbol{b}_3$ 的重量是3,从而 $W(\boldsymbol{x})+W(\boldsymbol{Ax})\geqslant1+3=4$;如果 $\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3$ 互不相等,则 $\boldsymbol{Ax}$ 的输出块 $\boldsymbol{e}_1\oplus\boldsymbol{e}_2,\boldsymbol{e}_2\oplus\boldsymbol{e}_3,\boldsymbol{e}_3\oplus\boldsymbol{e}_1$ 都非零,从而 $W(\boldsymbol{x})+W(\boldsymbol{Ax})\geqslant1+3=4$.

(2)设 $W(\boldsymbol{Ax})=1$,则 $\boldsymbol{A}^{-1}=\boldsymbol{M}_1^{-1}\boldsymbol{H}^{-1}\boldsymbol{M}_2^{-1}=\boldsymbol{M}_1^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{M}_2^{\mathrm{T}}$ 仍然是ARIA型扩散结构.令 $\boldsymbol{y}=\boldsymbol{Ax}$,则有 $\boldsymbol{x}=\boldsymbol{A}^{-1}\boldsymbol{y}$,故由(1)知

$$W(\boldsymbol{x})+W(\boldsymbol{Ax})=W(\boldsymbol{A}^{-1}\boldsymbol{y})+W(\boldsymbol{y})\geqslant4.$$

(3)设 $W(\boldsymbol{x})\geqslant2$. 如果 $W(\boldsymbol{x})\geqslant3$,则由 $\boldsymbol{Ax}\neq0$ 知 $W(\boldsymbol{x})+W(\boldsymbol{Ax})\geqslant3+1=4$. 如果 $W(\boldsymbol{x})=2$,假设 $W(\boldsymbol{Ax})=1$,则由(2)知 $W(\boldsymbol{x})+W(\boldsymbol{Ax})\geqslant4$,从而与 $W(\boldsymbol{x})=2$ 矛盾,该矛盾这说明 $W(\boldsymbol{Ax})\geqslant2$,因而有

$$W(\boldsymbol{x})+W(\boldsymbol{Ax})\geqslant2+2=4.$$

证毕

4.1 16阶ARIA型扩散结构的分支数

由第一层和第三层矩阵的选取不影响分支数,则不妨固定其为 $\boldsymbol{M}$;再由交换中间层矩阵的位置不影响分支数知,只需考察其一种排列即可.从而,研究ARIA型扩散结构的分支数,只需研究中间层的四个小块矩阵的以下三种情况:

(A)至少三个小块矩阵相同;

(B)有两个矩阵相同;

(C)互不相同.

对于(A),由4.2节定理6知,此时ARIA型扩散结构的分支数必为4. 对于(B),由定理3及定理4知,不妨设中间层第一个和第二个小块矩阵相同且为 $\boldsymbol{M}$,则只需考察第三个和第四个小块矩阵的选取,共 C_{23}^2+23 种;对于(C),不妨固定第一个小块矩阵为 $\boldsymbol{M}$,考察其余三个小块矩阵共 C_{23}^3 种;因此,最后需要考察的情况为 $C_{23}^2+23+C_{23}^3=2047$ 种.

引理5[8] 设 $\boldsymbol{A}$ 为 $\mathrm{GF}(2^s)$ 上的 n 维二元矩阵,$f:[\mathrm{GF}(2^{sm})]^n\rightarrow[\mathrm{GF}(2^{sm})]^n$ 定义为 $f(z)=\boldsymbol{Az}$,其中 $\boldsymbol{z}$ 是有限域 $\mathrm{GF}(2^{sm})$ 上的 n 维列向量,则对 $m\geqslant1$,都有 $D_f^{(s)}=D_f^{(sm)}$ 和 $L_f^{(s)}=L_f^{(sm)}$ 成立.

在引理5中取 $s=1$,则可将 $\mathrm{GF}(2^m)$ 上16阶ARIA型扩散结构的分支数计算,简化为计算 $\mathrm{GF}(2)$ 域上.

定理5 设线性变换 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 为 $\mathrm{GF}(2^m)$ 上的16阶ARIA型扩散结构,则 $\boldsymbol{A}$ 的分支数只能为4或8.

证明 通过上述分支数的等价分类,再利用下面的算法1可知,ARIA型扩散结构 $\boldsymbol{A}$ 的分支数只能为4或者8.

算法1 ARIA型扩散结构分支数搜索算法

```
输入:m_i, m_i^* ←0, 4≤i≤8//分支数为 i 的计数器
输出:m_i, m_i^*
set M_1 = M_2 = H_1 = H_2 = M
for(H_3→) for(H_4→)//穷举情况(B)
{
  a = getbranch(H_1, H_2, H_3, H_4)//计算分支数
  switch(a){                    //统计此时的分支数
    case 4: write(4, H_3, H_4), m_4 + +;
    case 5: write(5, H_3, H_4), m_5 + +;
    case 6: write(6, H_3, H_4), m_6 + +;
    case 7: write(7, H_3, H_4), m_7 + +;
    case 8: write(8, H_3, H_4), m_8 + +;}
}
for(H_2→) for(H_3→) for(H_4→)//穷举情况(C)
{
  a = getbranch(H_1, H_2, H_3, H_4)//计算分支数
  switch(a){ //统计此时的分支数
    case 4: write(4, H_2, H_3, H_4), m_4^* + +;
    case 5: write(5, H_2, H_3, H_4), m_5^* + +;
    case 6: write(6, H_2, H_3, H_4), m_6^* + +;
    case 7: write(7, H_2, H_3, H_4), m_7^* + +;
    case 8: write(8, H_2, H_3, H_4), m_8^* + +;}
}
```

实验结果表明,情况(B)和情况(C)分别有21种和848种不同的分支数为8的ARIA型扩散结构,其余ARIA型扩散结构的分支数均为4.

证毕

4.2 分支数为4的16阶ARIA型扩散结构

定理6 设线性变换 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 为 $\mathrm{GF}(2^m)$ 上的16阶ARIA型扩散结构,则 $\boldsymbol{A}$ 的分支数为4的充要条件是存在 $\mathrm{GF}(2^m)$ 上满足 $1\leqslant W(\boldsymbol{a})\leqslant2$ 的分量仅取0,1值的4维列向量 $\boldsymbol{a}$ 和 $1\leqslant i<j<k\leqslant4$,使得

$$\boldsymbol{H}_i\boldsymbol{a}=\boldsymbol{H}_j\boldsymbol{a}=\boldsymbol{H}_k\boldsymbol{a}.$$

证明 根据定理2,不妨设 $\boldsymbol{M}_1=\boldsymbol{M}_2=\boldsymbol{M}$.

充分性 设 $1\leqslant i<j<k\leqslant4$ 和分量仅取0,1值的4维列向量 $\boldsymbol{a}\in\{0,1\}^4$ 满足

$$1\leqslant W(\boldsymbol{a})\leqslant2\text{ 和 }\boldsymbol{H}_i\boldsymbol{a}=\boldsymbol{H}_j\boldsymbol{a}=\boldsymbol{H}_k\boldsymbol{a}.$$

由定理3知,不妨设 $\boldsymbol{H}_2\boldsymbol{a}=\boldsymbol{H}_3\boldsymbol{a}=\boldsymbol{H}_4\boldsymbol{a}$. 取 $\boldsymbol{x}$ 的第1块为 $\boldsymbol{a}$,其它3块都是4维全0向量,则由 $\boldsymbol{M}_1$ 的定义知,$\boldsymbol{H}_1$ 的输入为 $\boldsymbol{0}$ 且 $\boldsymbol{H}_2,\boldsymbol{H}_3,\boldsymbol{H}_4$ 的输入都是 $\boldsymbol{a}$,故 $\boldsymbol{H}_1$ 的输出是 $\boldsymbol{0}$,而 $\boldsymbol{H}_2,\boldsymbol{H}_3,\boldsymbol{H}_4$ 的输出相等. 故由 $\boldsymbol{M}_2$ 的定义知,$\boldsymbol{M}_2$ 的第1个输出块是 $\boldsymbol{H}_2\boldsymbol{a}\neq\boldsymbol{0}$,其它3块都是 $\boldsymbol{0}$,故有 $W(\boldsymbol{Ax})=W(\boldsymbol{H}_2\boldsymbol{a})$,于是有 $W(\boldsymbol{x})+W(\boldsymbol{Ax})=W(\boldsymbol{a})+W(\boldsymbol{H}_2\boldsymbol{a})$.

如果 $W(\boldsymbol{a})=1$,则由 $\boldsymbol{H}_2$ 的定义知 $W(\boldsymbol{H}_2\boldsymbol{a})=3$,此

时 $W(\boldsymbol{x})+W(\boldsymbol{Ax})=W(\boldsymbol{a})+W(\boldsymbol{H}_2\boldsymbol{a})=1+3=4$. 故由 $\boldsymbol{A}$ 的分支数≥4 知,此时 $\boldsymbol{A}$ 的分支数为 4.

如果 $W(\boldsymbol{a})=2$,则有 $W(\boldsymbol{H}_2\boldsymbol{a})=2$,此时 $W(\boldsymbol{x})+W(\boldsymbol{Ax})=W(\boldsymbol{a})+W(\boldsymbol{H}_2\boldsymbol{a})=2+2=4$. 故由 $\boldsymbol{A}$ 的分支数≥4 知,此时 $\boldsymbol{A}$ 的分支数为 4.

必要性　设 16 阶 ARIA 型扩散结构 $\boldsymbol{A}$ 的分支数为 4,则存在输入 $\boldsymbol{x}$,使得 $W(\boldsymbol{x})+W(\boldsymbol{Ax})=4$. 此时,有以下三种情况:

(1) $W(\boldsymbol{x})=1, W(\boldsymbol{Ax})=3$.

设 $\boldsymbol{x}$ 的 4 大块输入中,有一块是 $\boldsymbol{a}$,另外 3 块都是 $\boldsymbol{0}$,则有 $W(\boldsymbol{a})=1$,且对任意 $i\in\{1,2,3,4\}$,都有 $\boldsymbol{H}_i\boldsymbol{a}=3$. 根据 $\boldsymbol{M}_1$ 的定义,存在 $t\in\{1,2,3,4\}$,使得 $\boldsymbol{H}_t$ 的输入是 $\boldsymbol{0}$,且当 $i\in\{1,2,3,4\}\setminus\{t\}$ 时 $\boldsymbol{H}_i$ 的输入都是 $\boldsymbol{a}$. 记 $\{1,2,3,4\}=\{i,j,k,t\}$,则 $\boldsymbol{H}_t$ 的输出是 $\boldsymbol{0}$,且 $\boldsymbol{H}_i,\boldsymbol{H}_j,\boldsymbol{H}_k$ 的输出分别是 $\boldsymbol{H}_i\boldsymbol{a},\boldsymbol{H}_j\boldsymbol{a},\boldsymbol{H}_k\boldsymbol{a}$,根据 $\boldsymbol{M}_2$ 的定义,$\boldsymbol{M}_2$ 的四块输出分别是

$$\boldsymbol{H}_i\boldsymbol{a}\oplus\boldsymbol{H}_j\boldsymbol{a}\oplus\boldsymbol{H}_k\boldsymbol{a},\boldsymbol{H}_j\boldsymbol{a}\oplus\boldsymbol{H}_k\boldsymbol{a},\boldsymbol{H}_k\boldsymbol{a}\oplus\boldsymbol{H}_i\boldsymbol{a},\boldsymbol{H}_i\boldsymbol{a}\oplus\boldsymbol{H}_j\boldsymbol{a},$$

故由 $W(\boldsymbol{Ax})=3$ 知,上述 4 块中至少有 1 个是 $\boldsymbol{0}$.

当 $\boldsymbol{H}_i\boldsymbol{a}\oplus\boldsymbol{H}_j\boldsymbol{a}\oplus\boldsymbol{H}_k\boldsymbol{a}=\boldsymbol{0}$ 时,上述 4 块分别为 $\boldsymbol{0},\boldsymbol{H}_i\boldsymbol{a},\boldsymbol{H}_j\boldsymbol{a},\boldsymbol{H}_k\boldsymbol{a}$. 此时输出重量为

$$W(\boldsymbol{H}_i\boldsymbol{a})+W(\boldsymbol{H}_j\boldsymbol{a})+W(\boldsymbol{H}_k\boldsymbol{a})=3+3+3=9.$$

这与输出重量为 3 矛盾. 故 $\boldsymbol{H}_i\boldsymbol{a}\oplus\boldsymbol{H}_j\boldsymbol{a}\oplus\boldsymbol{H}_k\boldsymbol{a}\neq\boldsymbol{0}$,即上述第 2 块,第 3 块和第 4 块中至少有 1 个是 $\boldsymbol{0}$. 不妨设 $\boldsymbol{H}_i\boldsymbol{a}\oplus\boldsymbol{H}_j\boldsymbol{a}=\boldsymbol{0}$,则上述 4 块分别为

$$\boldsymbol{H}_k\boldsymbol{a},\boldsymbol{H}_j\boldsymbol{a}\oplus\boldsymbol{H}_k\boldsymbol{a},\boldsymbol{H}_k\boldsymbol{a}\oplus\boldsymbol{H}_i\boldsymbol{a},\boldsymbol{0}.$$

由 $W(\boldsymbol{H}_k\boldsymbol{a})=3, W(\boldsymbol{Ax})=3$ 知,$\boldsymbol{H}_k\boldsymbol{a}\oplus\boldsymbol{H}_i\boldsymbol{a}=\boldsymbol{0}$,

$\boldsymbol{H}_j\boldsymbol{a}\oplus\boldsymbol{H}_k\boldsymbol{a}=\boldsymbol{0}$,因而有 $\boldsymbol{H}_i\boldsymbol{a}=\boldsymbol{H}_j\boldsymbol{a}=\boldsymbol{H}_k\boldsymbol{a}$. 再设 $\boldsymbol{a}'$ 是将 $\boldsymbol{a}$ 的非零分量全部改为 1 所得的向量,则有 $W(\boldsymbol{a}')=W(\boldsymbol{a})=1$ 和 $\boldsymbol{H}_i\boldsymbol{a}'=\boldsymbol{H}_j\boldsymbol{a}'=\boldsymbol{H}_k\boldsymbol{a}'$,这说明此时必要性成立.

(2) $W(\boldsymbol{x})=3, W(\boldsymbol{Ax})=1$.

令 $\boldsymbol{A}^{-1}=\boldsymbol{M}_1^{-1}\boldsymbol{H}^{-1}\boldsymbol{M}_2^{-1}=\boldsymbol{M}_1^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{M}_2^{\mathrm{T}}$,则 $\boldsymbol{A}^{-1}$ 仍是 16 阶 ARIA 型扩散结构. 令 $\boldsymbol{y}=\boldsymbol{Ax}$,则有 $W(\boldsymbol{y})=1, W(\boldsymbol{A}^{-1}\boldsymbol{y})=3$,此时可以等价于(1).

(3) $W(\boldsymbol{x})=2, W(\boldsymbol{Ax})=2$.

按照输入 $\boldsymbol{x}$ 的重量分布可分为两类:(A)有两块分别为 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 且 $W(\boldsymbol{a})=W(\boldsymbol{b})=1$,另外 2 块都是 $\boldsymbol{0}$;(B)有一块是 $\boldsymbol{a}$ 且 $W(\boldsymbol{a})=2$,另外 3 块都是 $\boldsymbol{0}$. 对于情况(A),根据 $\boldsymbol{M}_1$ 的定义知,存在 $i,j\in\{1,2,3,4\}$,使得 $\boldsymbol{H}_i,\boldsymbol{H}_j$ 的输入分别为 $\boldsymbol{a}$ 和 $\boldsymbol{b}$,则 $\boldsymbol{H}_i,\boldsymbol{H}_j$ 的输出分别为 $\boldsymbol{H}_i\boldsymbol{a},\boldsymbol{H}_j\boldsymbol{b}$,且有 $W(\boldsymbol{H}_i\boldsymbol{a})=W(\boldsymbol{H}_j\boldsymbol{b})=3$,即 $\boldsymbol{M}_2$ 的输入必有两块重量为 3. 另一方面,由 $\boldsymbol{M}_2$ 的输出重量为 $W(\boldsymbol{Ax})=2$ 且 $\boldsymbol{M}_2^{-1}=\boldsymbol{M}_2$,再根据 $\boldsymbol{M}_2^{-1}$ 仅在对角线上为全 0 阵,其余都是单位阵,讨论 $\boldsymbol{M}_2$ 的输出重量分布情况,可得 $\boldsymbol{M}_2$ 的输入重量≤2,这与 $\boldsymbol{M}_2$ 的输入必有两块重量为 3 矛盾. 因此,分支数为 4 且 $W(\boldsymbol{x})=2, W(\boldsymbol{Ax})=2$ 时,$\boldsymbol{x}$ 的重量分布只可能为情况(B). 而对于情况(B),只是 $\boldsymbol{a}$ 的重量不同,证明完全可以归结为(1),此时必要性成立.

证毕

4.3　分支数为 8 的 16 阶 ARIA 型扩散结构的充要条件、计数问题及对合构造

由 ARIA 型扩散结构的分支数只能为 4 或 8,再结合定理 6 分支数为 4 的充要条件,即得定理 7.

定理 7　设线性变换 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 是 $\mathrm{GF}(2^m)$ 上的 16 阶 ARIA 型扩散结构,则 $\boldsymbol{A}$ 的分支数为 8 的充要条件是不存在 $\mathrm{GF}(2^m)$ 上满足 $1\leqslant W(\boldsymbol{a})\leqslant 2$ 的分量仅取 0,1 值的 4 维列向量 $\boldsymbol{a}$ 和 $1\leqslant i<j<k\leqslant 4$,使得

$$\boldsymbol{H}_i\boldsymbol{a}=\boldsymbol{H}_j\boldsymbol{a}=\boldsymbol{H}_k\boldsymbol{a}.$$

由此给出算法 2.

算法 2　分支数为 8 的 16 阶 ARIA 型扩散结构构造算法

输入:分支数为 4 的 4 级二元方阵
输出:分支数为 8 的 16 级 ARIA 型扩散结构
步骤 1:任意挑选分支数为 4 的 4 级二元方阵
　　作为第一、三层线性变换.
步骤 2:挑选四个分支数为 4 的 4 级二元方阵,
　　若所有情况挑选完毕,则执行步骤 1,
　　否则执行步骤 3.
步骤 3:依次挑选步骤 2 中三个矩阵,
　　检查每一列是否相同,
　　若相同则跳转步骤 2,否则执行步骤 4.
步骤 4:依次挑选三个小块矩阵,挑选其中两列,
　　分别进行异或加,检查是否相同,
　　若相同则跳转步骤 2,否则执行步骤 5.
步骤 5:输出此时构造的 ARIA 型扩散结构.

由算法 2 可知,一个分支数为 8 的 16 阶 ARIA 型扩散结构需要通过 $C_4^3\cdot(C_4^1+C_4^2)=40$ 次检测,其计算复杂度可忽略不计. 而随机生成 10^6 个 16 阶可逆二元方阵,未发现分支数为 8 的矩阵. 因此说明构造算法 2 非常有效.

定理 8　设线性变换 $\boldsymbol{A}=\boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 为 $\mathrm{GF}(2^m)$ 上的 16 阶 ARIA 型扩散结构,则共有 12013056 种不同的分支数为 8 的 ARIA 型扩散结构.

证明　由定理 5 知,算法 1 共有 869 种不同的分支数为 8 的 ARIA 型扩散结构,从而由定理 4 知,遍历列变换 θ 的 24 种可能,可得中间层的构造方法共有 20856 种. 再结合定理 2,最终可构造 $24\times 24\times 20856=12013056\approx 2^{23.52}$ 个不同的分支数为 8 的 ARIA 型扩散结构.

证毕

下面由定理 1 的(2),构造分支数为 8 的 16 阶对合 ARIA 型扩散结构. 首先,构造中间层,从算法 1 分支数

为 8 的 ARIA 型扩散结构中,统计中间层矩阵均为对合矩阵的个数,然后由定理4,遍历列变换 θ 的24 种可能,再分别统计中间层矩阵均为对合矩阵的个数,最后总数为 388 种;其次,第一层和第三层的选取满足 $\boldsymbol{M}_1 = \boldsymbol{M}_2^{-1}$,可选取有 24 对. 最终可构造 $388 \times 24 = 9312$ 个分支数为 8 的 16 阶对合 ARIA 型扩散结构.

最后,给出一个分支数为 8 的 16 阶对合 ARIA 型扩散结构的实例. 令 $\boldsymbol{M}_1 = \boldsymbol{M}_2 = \boldsymbol{M}$,设 $\boldsymbol{H}_1, \boldsymbol{H}_2, \boldsymbol{H}_3, \boldsymbol{H}_4$ 的矩阵分别为

$$\boldsymbol{H}_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}, \boldsymbol{H}_2 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix},$$

$$\boldsymbol{H}_3 = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}, \boldsymbol{H}_4 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix},$$

则此时的扩散结构 $\boldsymbol{A} = \boldsymbol{M}_2\boldsymbol{H}\boldsymbol{M}_1$ 为分支数为 8 的 16 阶对合 ARIA 型扩散结构且表示为

$$\boldsymbol{A} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

5 总结

本文提出了 ARIA 型扩散结构的定义,证明了对 ARIA 型扩散结构做以下三种变换后分支数不变且仍为 ARIA 型扩散结构:(1)对 ARIA 型扩散结构的输入和输出复合块移位变换;(2)交换中间层矩阵的位置;(3)对中间层矩阵的输入和输出分别复合相同的移位变换. 其次,证明了 ARIA 型扩散结构是正交矩阵. 最后,给出了分支数为 8 的 16 阶 ARIA 型扩散结构的充要条件以及分支数为 8 的 16 阶对合 ARIA 型扩散结构的构造方法.

本文重点研究了 16 阶 ARIA 型扩散层的结构特点,下一步可继续研究 32 阶 ARIA 型扩散层的结构特点. 其次,复合型扩散结构在实现上有着天然的优势,利用其它复合结构构造扩散层将是下一步的研究方向.

参考文献

[1] Xiao L, Heys H M. Hardware design and analysis of block cipher components [J]. Lecture Notes in Computer Science, 2002, 2587: 164 – 181.

[2] NTT-Nippon Telegraph and Telephone Corporation. E2: a 128-Bit Block Cipher [EB/OL]. http://info.isl.ntt.co.jp/e2. 2007.

[3] Aoki K, Ichikawa T, Kanda M, et al. Camellia: a 128-bit block cipher suitable for multiple platforms [A]. Douglas R. Selected Areas in Cryptography-SAC 2000 [C]. Canada: Springer-Verlag, 2000. 41 – 54.

[4] Kwon D, Kim J, Park S, et al. New block cipher: ARIA [A]. Lim J I. International Conference on Information Security and Cryptology-ICISC 2003 [C]. Berlin: Springer-Verlag, 2003. 432 – 445.

[5] Kang Ju-sung. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks[J]. ETRI Journal, 2001, 23(4): 158 – 167.

[6] 吴文玲,冯登国,张文涛. 分组密码的设计与分析[M]. 北京:清华大学出版社,2009. 240 – 245.

[7] Bon Wook Koo, Hwan Seok Jang, Jung Hwan Song. On constructing of a 32 × 32 binary matrix as a diffusion layer for a 256-bit block cipher[A]. Min S R. International Conference on Information Security and Cryptology-ICISC 2006[C]. Berlin: Springer-Verlag, 2006. 51 – 64.

[8] 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.
Cui T, Chen H S, Jin C H. Several properties of binary diffusion layers for block cipher [J]. Journal of Software, 2012, 23(9): 2430 – 2437. (in Chinese)

[9] 郭磊,郑浩然,刘明伟. 一类具有最大分支数的 16 阶 0 – 1 矩阵构造[J]. 计算机工程,2013,39(12):118 – 121.
Guo L, Zheng H R, Liu M W. A class of 16-order 0-1 matrix construction with the largest number of branches[J]. Computer Engineering and Applications, 2013, 39(12): 118 – 121. (in Chinese)

[10] Sakalli M T, Aslan B. On the algebraic construction of cryptographically good 32 × 32 binary linear transformations[J]. Security and Communication Networks, 2014, 259(1): 485 – 494.

[11] Akleylek S, Rijmen V, Sakallinodot, et al. Efficient methods to generate cryptographically significant binary diffusion layers[J]. IET Information Security, 2017, 11(4):

177 – 187.

[12] Akleylek S, Sakalli M T, Ozturk E, et al. Generating binary diffusion layers with maximum/high branch numbers and low search complexity[J]. Security and Communication Networks, 2016, 9(16): 3558 – 3569.

[13] Koo B W, Jang H S, Song J H. Constructing and cryptanalysis of a 16 × 16 binary matrix as a diffusion layer [A]. Kijoon C. Information Security Applications: 4th International Workshop-WISA 2003 [C]. Berlin: Springer-Verlag, 2003. 489 – 503.

[14] Daemen J. Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis[D]. Belgium: Catholic University of Louvain, 1995. 101 – 103.

作者简介

马宿东　男,1995 年 8 月出生于安徽宿州. 现为信息工程大学硕士研究生. 从事对称密码相关研究.
E-mail:1668945764@qq.com

金晨辉　男,信息工程大学教授、博士生导师. 1965 年 3 月出生于河南扶沟. 研究方向为密码学与信息安全.
E-mail:jinchenhui@126.com

关　杰　女,信息工程大学教授、博士生导师. 1974 年 9 月生于河南郑州. 研究方向为对称密码的设计与分析.
E-mail:guanjie007@163.com