软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(9):2430−2437 [doi: 10.3724/SP.J.1001.2012.04137]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

分组密码二元扩散结构的几点注记*

崔 霆[1+], 陈河山[2], 金晨辉[1]

[1](信息工程大学 电子技术学院,河南 郑州 450004)

[2](河南大学,河南 开封 475001)

Several Properties of Binary Diffusion Layers for Block Cipher

CUI Ting[1+], CHEN He-Shan[2], JIN Chen-Hui[1]

[1](Institution of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

[2](He'nan University, Kaifeng 475001, China)

+ Corresponding author: E-mail: cuiting_1209@yahoo.com.cn

Cui T, Chen HS, Jin CH. Several properties of binary diffusion layers for block cipher. *Journal of Software*, 2012,23(9):2430−2437 (in Chinese). http://www.jos.org.cn/1000-9825/4137.htm

Abstract: 0-1 matrices are often-used in the design of diffusion structures in block ciphers. This paper first proves that the branch number of matrix over $GF(2^n)$ does not change while it is redefined over the extension field $GF(2^{mn})$. By this result, the study reinforces the proof given by Choy *et al*., which is about the upper bound of branch number of binary matrices over $GF(2^n)$. This paper constructs a kind of invertible binary matrices with size 8 and largest branch number, proposes a kind of matrices with equal differential branch number and linear branch number, and also includes lots of matrices and involution matrices with order 16 and optimal branch number with this structure are searched out.

Key words: block cipher; diffusion structure; branch number; 0-1 matrices

摘 要: 0-1 矩阵常用于设计分组密码的扩散结构.首先证明,当 $GF(2^n)$上的矩阵重新定义在扩域 $GF(2^{mn})$上时其分支数保持不变,据此补充了 Choy 等人关于 $GF(2^n)$上二元矩阵分支数上界的证明.构造了一批分支数达到最优的 8 阶二元可逆矩阵,给出了一类差分分支数和线性分支数相等的二元可逆矩阵,并从中搜索出了大量 16 阶分支数达到最优的二元矩阵和对合二元矩阵.

关键词: 分组密码;扩散结构;分支数;0-1 矩阵

中图法分类号: TN309 **文献标识码**: A

扩散结构是分组密码的关键环节之一,其对分组密码的安全性和实现效率有着直接影响.Rijmen 提出差分分支数与线性分支数的概念度量扩散结构的扩散效果[1].使用 $GF(2^n)$上的矩阵可以设计出分支数达到最大的扩散结构,然而这样的设计在实现时通常需要处理有限域的乘法[2],如果利用二元矩阵设计扩散结构,虽然这一类扩散结构的分支数不能达到最大值,但是仅采用少量的异或操作便可完成算法的扩散过程,因而非常利于密码算法的实现[3−6].近年出现的分组密码算法,如 E2[3],Camellia[4],ARIA[5]等,均采用了 8 阶或 16 阶 0-1 矩阵来设

* 基金项目: 国家自然科学基金(61272488, 60272041)
收稿时间: 2011-03-22; 修改时间: 2011-09-02; 定稿时间: 2011-10-17

计扩散结构.因此,研究$GF(2^n)$上二元矩阵分支数的特性,以及分支数达到最优的二元矩阵的构造,对于密码算法的设计有现实的意义.

目前,在该领域还有许多问题需要解决:

首先,有限域上的二元矩阵分支数是否就是该矩阵在二元域上的分支数,目前尚无明确结论.如果该问题有肯定的答案,将为二元矩阵的分支数分析及分支数达到最大的二元矩阵的构造带来较大的便利.由于没有该结论保障,文献[6]中关于有限域上二元矩阵分支数上界的证明是有缺陷的.

其次,由于常见的分组密码的分组长度为 128bit 或 64bit,而一般采用的 S 盒多为 8bit,故而给出阶数为 8 和 16,且分支数达到最优的二元矩阵是具备实用意义的.在密码算法的实现中,设计者甚至希望矩阵满足对合性,从而简化逆矩阵的实现,节省加脱密算法的实现开销.在矩阵阶较小时,可以通过随机搜索来构造出分支数最优的二元矩阵;然而当矩阵阶较大时,直接搜索是不现实的(对可逆的 8 阶和 16 阶二元矩阵,作者分别随机检测了10^8 例,未能找到分支数达到最大的二元矩阵).文献[7]通过对搜索空间加以限制,构造了一批分支数达到最大的二元矩阵.然而该文献仅考察了矩阵的差分分支数,并未兼顾线性分支数.文献[5,8]各自提供了一例分支数达到最大的 16 阶对合二元矩阵.

此外,矩阵的分支数达到最优的前提是差分分支数与线性分支数相等,因此要研究最优二元矩阵的构造,最好事先构造差分分支数与线性分支数相等的矩阵.

本文将研究上述问题.首先证明了将$GF(2^n)$上矩阵视为扩域$GF(2^{mn})$上的矩阵时二者分支数相等.利用这一结果,本文补充了文献[6]的相关证明;其后还给出一类阶为 8 且差分分支数与线性分支数均达到最大的 0-1 矩阵的构造方法;最后,本文构造了一类差分分支数和线性分支数相等的矩阵,并从中搜索所有分支数达到最大的 16 阶 0-1 矩阵.实验结果说明,从此类矩阵中搜索分支数达到最优的二元矩阵比随机搜索的成功率大得多.

1 准备工作

本文均用⊕表示逐位模 2 加,用+表示实数加,用A^T表示矩阵或向量A的转置.对$y=(y_1,y_2,\ldots,y_m)\in GF(2^n)^m$,均以$W_n(y)$表示$y_1,y_2,\ldots,y_m$中非 0 元的个数.若$y$是行向量,令$y>>>t=(y_{m-t+1},\ldots,y_m,y_1,\ldots,y_{m-t})$;若$y$是列向量,令$y>>>t=(y^T>>>t)^T$.用$M>>>t$表示将矩阵$M$的每行均循环右移$t$位.

定义 1[9]. 设$f:[GF(2^n)]^m\to[GF(2^n)]^m$是有限域$GF(2^n)$上的多输出线性映射,若$f(x)=Ax$,$A$是$GF(2^n)$上的$m\times m$矩阵,则$A$的差分分支数定义为

$$D_f^{(n)}=\min\{W_n(\alpha)+W_n(A\alpha):\alpha\in[GF(2^n)]^m\setminus\{0\}\},$$

其线性分支数定义为

$$L_f^{(n)}=\min\{W_n(A^T\alpha)+W_n(\alpha):\alpha\in[GF(2^n)]^m\setminus\{0\}\}.$$

这里,α为$GF(2^n)$上的m维列向量.

由定义 1 立即有:

定理 1. 设M为$GF(2^n)$上的$m\times m$矩阵,$f:[GF(2^{ns})]^m\to[GF(2^{ns})]^m$定义为$f(z)=Mz$,其中,$z$是有限域$GF(2^{ns})$上的$m$维列向量,则对$s\geqslant 1$,都有$D_f^{(n)}=D_f^{(ns)}$和$L_f^{(n)}=L_f^{(ns)}$成立.

证明:仅对差分分支数的情形加以证明.线性分支数的情形可类似得到.

由定义 1 得知$D_f^{(ns)}=\min\{W_{ns}(x)+W_{ns}(Mx):x\in[GF(2^{ns})]^m\setminus\{0\}\}$.以下证明$D_f^{(n)}=D_f^{(ns)}$.因$GF(2^{ns})$是$GF(2^n)$上的$s$维线性空间,故可取定一组基$\alpha_0,\alpha_1,\ldots,\alpha_{s-1}$,则对$\forall\alpha\in GF(2^{ns})$可以唯一表示为$\alpha=z_0\alpha_0\oplus\ldots\oplus z_{s-1}\alpha_{s-1}$.

这里,对$0\leqslant i\leqslant s-1$,均有$z_i\in GF(2^n)$.

记$M=(m_{i,j})$,设$[GF(2^{ns})]^m\setminus\{0\}$中的元素$x=(x_0,\ldots,x_{m-1})^T$满足$W_{ns}(x)+W_{ns}(Mx)=D_f^{(ns)}$,令$[GF(2^{ns})]^m$上的列向量$y=(y_0,\ldots,y_{m-1})^T$满足$y=Mx$.因$y_i,x_i\in GF(2^{ns})$,故设$y_i=\bigoplus_{t=0}^{s-1}y_{i,t}\cdot\alpha_t$,$x_i=\bigoplus_{t=0}^{s-1}x_{i,t}\cdot\alpha_t$.若假设对$\forall 0\leqslant i\leqslant m-1,0\leqslant t\leqslant s-1$均有$x_{i,t}=0$,则诸$x_i=0$,即$x=0$,这与条件矛盾.因而一定存在某个$0\leqslant t_0\leqslant s-1$,使得$x'=(x_{0,t_0},\ldots,x_{m-1,t_0})^T\neq 0$.

由 $x_i=\bigoplus_{t=0}^{s-1}x_{i,t}\cdot\alpha_t$ 以及 $y_i=\bigoplus_{k=0}^{m-1}m_{i,k}x_k$ 知 $y_i=\bigoplus_{k=0}^{m-1}m_{i,k}x_k=\bigoplus_{k=0}^{m-1}m_{i,k}\bigoplus_{t=0}^{s-1}x_{k,t}\cdot\alpha_t=\bigoplus_{t=0}^{s-1}\bigoplus_{k=0}^{m-1}m_{i,k}x_{k,t}\cdot\alpha_t$,同时有 $y_i=\bigoplus_{t=0}^{s-1}y_{i,t}\cdot\alpha_t$. 根据代数学知识可知,$y_i$ 被基 $\alpha_0,\alpha_1,\ldots,\alpha_{s-1}$ 唯一表出,因而对 $\forall 0\leqslant t\leqslant s-1$,均有 $y_{i,t}=\bigoplus_{k=0}^{m-1}m_{i,k}x_{k,t}$,故 $y_{i,t_0}=\bigoplus_{k=0}^{m-1}m_{i,k}x_{k,t_0}$ 也成立.

令 $y'=(y_{0,t_0},y_{1,t_0},\ldots,y_{m-1,t_0})^T$,由上可知 $y'=Mx',x',y'\in[GF(2^n)]^m$ 和 $x'\neq 0$.显然有 $W_{ns}(x)\geqslant W_n(x')$ 和 $W_{ns}(y)\geqslant W_n(y')$, 故 $D_f^{(ns)}=W_{ns}(x)+W_{ns}(y)\geqslant W_n(x')+W_n(y')\geqslant D_f^{(n)}$; 反之,若 $x,y\in[GF(2^n)]^m$ 使得 $x\neq 0,y=Mx$ 和 $W_n(x)+W_n(y)=D_f^{(n)}$.

由于 $GF(2^n)$是 $GF(2^{ns})$的子域,因而有 $x,y\in[GF(2^{ns})]^m$ 且 $W_n(x)=W_{ns}(x),W_n(y)=W_{ns}(y)$,从而

$$D_f^{(ns)}\leqslant W_{ns}(x)+W_{ns}(y)=W_n(x)+W_n(y)=D_f^{(n)}.$$

即 $D_f^{(n)}=D_f^{(ns)}$. □

由定理 1 立即有:

推论 1.1. $GF(2)$上矩阵的分支数在其扩域 $GF(2^n)$上保持不变.

根据推论 1.1,下文在考察 0-1 矩阵时均在 $GF(2)$中考虑.Choy 等人在文献[6]中指出,$GF(2^n)$上 n 阶 0-1 矩阵的分支数上界为 $\left\lfloor\frac{2n+4}{3}\right\rfloor$,但该结论的证明存在缺陷,由于没有推论 1.1 的保障,实际上只证明了 $GF(2)$的情形.

由推论 1.1 立即有:

推论 1.2. $GF(2^n)$上 n 阶 0-1 矩阵的上界为 $\left\lfloor\frac{2n+4}{3}\right\rfloor$.

2 8 阶分支数为 5 的 0-1 矩阵的一类构造方法

8 阶 0-1 矩阵的分支数的上确界为 5[9],定理 2 给出了阶为 8、差分分支数与线性分支数均为 5 的二元矩阵的一种构造.

定理 2. 设 $a,b,c,d\in\{0,1\},a+b+c+d=3$,令 $M=\begin{pmatrix}a&b&c&d\\d&a&b&c\\c&d&a&b\\b&c&d&a\end{pmatrix}$,$\forall x,y\in\{0,1,2,3\}$,有

$$T_1=\begin{pmatrix}M & M>>>x\\ M>>>y & [M>>>(x+y)]\oplus[M>>>((x+y+1)\bmod 2)]\end{pmatrix}$$

和

$$T_2=\begin{pmatrix}M & M>>>x\\ M>>>y & [M>>>(x+y)]\oplus[M>>>((x+y+1)\bmod 2+2)]\end{pmatrix}$$

均可逆,且其差分分支数与线性分支数均为 5.

证明将分 3 步完成,即 T_1 和 T_2 可逆;T_1 和 T_2 的差分分支数为 5;T_1 和 T_2 的差分分支数等于线性分支数.

(1) T_1 和 T_2 可逆.

$\forall 0\leqslant x,y\leqslant 3$ 均有

$$|T_1|=\begin{vmatrix} M & M>>>x \\ M>>>y & [M>>>(x+y)]\oplus[M>>>((x+y+1)\bmod 2)] \end{vmatrix}$$

$$=\begin{vmatrix} M & M>>>x \\ 0 & [(M>>>x)>>>y]\oplus[M>>>(x+y)]\oplus[M>>>((x+y+1)\bmod 2)] \end{vmatrix}$$

$$=\begin{vmatrix} M & M>>>x \\ 0 & [M>>>(x+y)]\oplus[M>>>(x+y)]\oplus[M>>>((x+y+1)\bmod 2)] \end{vmatrix}$$

$$=\begin{vmatrix} M & M>>>x \\ 0 & [M>>>((x+y+1)\bmod 2)] \end{vmatrix}=|M||M>>>((x+y+1)\bmod 2)|=|M|^2\neq 0.$$

同样,

$$|T_2|=\begin{vmatrix} M & M>>>x \\ 0 & [M>>>(x+y)]\oplus[M>>>(x+y)]\oplus[M>>>((x+y+1)\bmod 2+2)] \end{vmatrix}$$

$$=\begin{vmatrix} M & M>>>x \\ 0 & [M>>>((x+y+1)\bmod 2+2)] \end{vmatrix}=|M||M>>>((x+y+1)\bmod 2+2)|=|M|^2\neq 0.$$

故 T_1 和 T_2 可逆.

(2) T_1 和 T_2 的差分分支数为 5.

因为 8 阶 0-1 矩阵的分支数不超过 5,故只需证明 T_1 和 T_2 的差分分支数不小于 5.为方便起见,记

$$N=[M>>>(x+y)]\oplus[M>>>((x+y+1)\bmod 2)],$$

$$Q=[M>>>(x+y)]\oplus[M>>>((x+y+1)\bmod 2+2)].$$

此时,必然有 $x+y\neq(x+y+1)\bmod 2$ 和 $x+y\neq(x+y+1)\bmod 2+2$,故 N 与 Q 均是每列(行)重量均为 2 的矩阵.为方便,此处的证明均以 $W(\cdot)$代替 $W_1(\cdot)$.

对$\forall\alpha=(\alpha_0,\ldots,\alpha_3,\alpha_4,\ldots,\alpha_7)^T\neq(0,\ldots,0)^T$,令$\alpha'=(\alpha_0,\ldots,\alpha_3)^T$,$\alpha''=(\alpha_4,\ldots,\alpha_7)$,则按照$\alpha$的重量 $W(\alpha)$进行分类讨论.

(2.1) $W(\alpha)=1$.此时,仅 $W(\alpha')=1$ 或 $W(\alpha'')=1$ 之一成立:

当 $W(\alpha')=1$ 时,由 $W(a,b,c,d)=3$ 知,$W(T_1\alpha)=W(T_2\alpha)=W(M\alpha')+W[(M>>>y)\alpha']=6$.

当 $W(\alpha'')=1$ 时:

$$W(T_1\alpha)=W[(M>>>x)\alpha'']+W(N\alpha'')=3+2=5,$$

$$W(T_2\alpha)=W[(M>>>x)\alpha'']+W(Q\alpha'')=3+2=5.$$

故当 $W(\alpha)=1$ 时,$W(\alpha)+W(T_1\alpha)\geqslant 5$,$W(\alpha)+W(T_2\alpha)\geqslant 5$.

(2.2) $W(\alpha)=2$.此时,$W(\alpha')=2$ 或 $W(\alpha'')=2$ 或 $W(\alpha')=W(\alpha'')=1$ 之一成立:

当 $W(\alpha')=2$ 时,有 $W(\alpha'')=0$,此时

$$W(T_2\alpha)=W(T_1\alpha)=W(M\alpha')+W[(M>>>y)\alpha']=2+2=4.$$

当 $W(\alpha'')=2$ 时,有 $W(\alpha')=0$.此时

$$W(T_1\alpha)=W[(M>>>x)\alpha'']+W(N\alpha''),$$

$$W(T_2\alpha)=W[(M>>>x)\alpha'']+W(Q\alpha'').$$

而不难验证 N 及 Q 的任意两列逐位模 2 和之后的重量均为 2,故 $W(T_1\alpha)=4$,$W(T_2\alpha)=4$.

当 $W(\alpha')=W(\alpha'')=1$ 时,因$(M>>>x)\alpha''=M(\alpha''<<<x)$(这里),故有:

$$W(T_1\alpha)=W[M(\alpha'\oplus(\alpha''<<<x))]+W[(M>>>y)\alpha'\oplus N\alpha'']$$

和

$$W(T_2\alpha)=W[M(\alpha'\oplus(\alpha''<<<x))]+W[(M>>>y)\alpha'\oplus Q\alpha''].$$

若$\alpha'\oplus(\alpha''<<<x)=0$,则有

$$W(T_1\alpha)=W[(M>>>y)(\alpha''<<<x)\oplus N\alpha'']=W[((M>>>(x+y))\oplus N)\alpha''].$$

由 N 矩阵的定义,$W(T_1\alpha)=W[(M>>>(x+y+1)\bmod 2)\alpha'']=3$.

类似有

$$W(T_2\alpha)=W[(M>>>y)(\alpha''<<<x)\oplus Q\alpha'']=W[((M>>>(x+y))\oplus Q)\alpha''].$$

由 Q 矩阵的定义,$W(T_2\alpha)=W[(M>>>((x+y+1) \bmod 2+2))\alpha'']=3$.

若$\alpha'\oplus(\alpha''<<<x)\neq 0$,可设$\alpha'=\alpha''<<<z$,显然,$x\neq z$,$W[(M(\alpha'\oplus(\alpha''<<<x)))=2$.

$$\begin{aligned}W[(M>>>y)\alpha'\oplus N\alpha'']&=W[(M>>>y)(\alpha''<<<z)\oplus N\alpha'']\\&=W[\{M>>>(y+z)\oplus M>>>(x+y)\oplus M>>>(x+y+1) \bmod 2\}\alpha'']\\&=W[M\{\alpha''<<<(y+z)\oplus\alpha''<<<(x+y)\oplus\alpha''<<<(x+y+1) \bmod 2\}].\end{aligned}$$

同时,

$$\begin{aligned}W[(M>>>y)\alpha'\oplus Q\alpha'']&=W[(M>>>y)(\alpha''<<<z)\oplus Q\alpha'']\\&=W[\{M>>>(y+z)\oplus M>>>(x+y)\oplus M>>>((x+y+1) \bmod 2+2)\}\alpha'']\\&=W[M\{\alpha''<<<(y+z)\oplus\alpha''<<<(x+y)\oplus\alpha''<<<((x+y+1) \bmod 2+2)\}].\end{aligned}$$

由 $y+z\neq x+y$ 和 $W(\alpha'')=1$ 知 $W[\alpha''<<<(y+z)\oplus\alpha''<<<(x+y)]=2$,因此,

$$\alpha''<<<(y+z)\oplus\alpha''<<<(x+y)\oplus\alpha''<<<(x+y+1) \bmod 2\neq 0,$$

$$\alpha''<<<(y+z)\oplus\alpha''<<<(x+y)\oplus\alpha''<<<((x+y+1) \bmod 2+2)\neq 0.$$

注意到 M 为可逆矩阵,故 $W[(M>>>y)\alpha'\oplus N\alpha'']\geqslant 1$,$W[(M>>>y)\alpha'\oplus Q\alpha'']\geqslant 1$.此时有:

$$W(T_1\alpha)=W[M(\alpha'\oplus(\alpha''<<<x))]+W[(M>>>y)\alpha'\oplus N\alpha'']\geqslant 3,$$

$$W(T_2\alpha)=W[M(\alpha'\oplus(\alpha''<<<x))]+W[(M>>>y)\alpha'\oplus Q\alpha'']\geqslant 3.$$

故当 $W(\alpha)=2$ 时,$W(\alpha)+W(T_1\alpha)\geqslant 5$,$W(\alpha)+W(T_2\alpha)\geqslant 5$.

(2.3) $W(\alpha)=3$.此时,$W(\alpha')=3$,或 $W(\alpha'')=3$,或 $W(\alpha')=1$,$W(\alpha'')=2$ 或 $W(\alpha')=2$,$W(\alpha'')=1$.

当 $W(\alpha')=3$ 时,有 $W(\alpha'')=0$,此时,$W(T_2\alpha)=W(T_1\alpha)=W(M\alpha')+W[(M>>>y)\alpha']=2$;

当 $W(\alpha'')=3$ 时,有 $W(\alpha')=0$,此时成立:

$$W(T_1\alpha)=W[(M>>>x)\alpha'']+W(N\alpha'')$$

和

$$W(T_2\alpha)=W[(M>>>x)\alpha'']+W(Q\alpha'').$$

注意到,N 矩阵及 Q 矩阵的 4 列列向量作逐位模 2 和为 0 之后重量为 0,且 N 矩阵及 Q 矩阵的每一列重量均为 2,故 N 矩阵及 Q 矩阵的任意 3 列列向量逐位模 2 和之后重量为 2.因此有 $W(N\alpha'')=2$ 和 $W(Q\alpha'')=2$.故

$$W(T_1\alpha)\geqslant 2+1=3,W(T_2\alpha)\geqslant 2+1=3.$$

当 $W(\alpha')=1$,$W(\alpha'')=2$ 或者 $W(\alpha')=2$,$W(\alpha'')=1$,此时有:

$$W(T_1\alpha)=W[M(\alpha'\oplus(\alpha''<<<x))]+W[(M>>>y)\alpha'\oplus N\alpha'']$$

和

$$W(T_2\alpha)=W[M(\alpha'\oplus(\alpha''<<<x))]+W[(M>>>y)\alpha'\oplus Q\alpha''].$$

又此时 $W[\alpha'\oplus(\alpha''<<<x)]$不可能为 2 和 4,以下分类讨论.

若 $W[\alpha'\oplus(\alpha''<<<x)]=1$,则有

$$W(T_1\alpha)\geqslant W[M(\alpha'\oplus(\alpha''<<<x))]=3,$$

$$W(T_2\alpha)\geqslant W[M(\alpha'\oplus(\alpha''<<<x))]=3.$$

若 $W[\alpha'\oplus(\alpha''<<<x)]=3$,则有 $W[M(\alpha'\oplus(\alpha''<<<x))]=1$,同时有:

$$\begin{aligned}(M>>>y)\alpha'\oplus N\alpha''&=(M>>>y)\alpha'\oplus[M>>>(x+y)]\alpha''\oplus[M>>>(x+y+1) \bmod 2]\alpha''\\&=M[(\alpha'<<<y)\oplus(\alpha''<<<(x+y))\oplus(\alpha''<<<(x+y+1) \bmod 2)]\end{aligned}$$

和

$$\begin{aligned}(M>>>y)\alpha'\oplus Q\alpha''&=(M>>>y)\alpha'\oplus[M>>>(x+y)]\alpha''\oplus[M>>>((x+y+1) \bmod 2+2)]\alpha''\\&=M[(\alpha'<<<y)\oplus(\alpha''<<<(x+y))\oplus(\alpha''<<<((x+y+1) \bmod 2+2))]\end{aligned}$$

成立.由 M 可逆,以下只需证明:

$$[\alpha'<<<y]\oplus[\alpha''<<<(x+y)]\oplus[\alpha''<<<(x+y+1) \bmod 2]\neq 0$$

与

$$[\alpha'<<<y]\oplus[\alpha''<<<(x+y)]\oplus[\alpha''<<<((x+y+1) \bmod 2+2)]\neq 0.$$

当 $W(\alpha')=1, W(\alpha'')=2$.

因 $x+y\neq(x+y+1)\bmod 2$ 和 $x+y\neq(x+y+1) \bmod 2+2$,故

$$W[(\alpha''<<<(x+y))\oplus(\alpha''<<<(x+y+1) \bmod 2)]$$

与

$$W[(\alpha''<<<(x+y))\oplus(\alpha''<<<((x+y+1) \bmod 2+2))]$$

必为偶数,因 $W(\alpha'<<<y)=1$,故此时有

$$[\alpha'<<<y]\oplus[\alpha''<<<(x+y)]\oplus[\alpha''<<<(x+y+1) \bmod 2]\neq 0$$

与

$$[\alpha'<<<y]\oplus[\alpha''<<<(x+y)]\oplus[\alpha''<<<((x+y+1) \bmod 2+2)]\neq 0.$$

当 $W(\alpha')=2$ 且 $W(\alpha'')=1$.

因 $W[\alpha'\oplus(\alpha''<<<x)]=3$,故

$$W[\alpha'\oplus(\alpha''<<<x)]=W[(\alpha'<<<y)\oplus(\alpha''<<<(x+y))]=3.$$

同时,

$$W[\alpha''<<<(x+y+1) \bmod 2]=W[\alpha''<<<((x+y+1) \bmod 2+2)]=1.$$

故有

$$[\alpha'<<<y]\oplus[\alpha''<<<(x+y)]\oplus[\alpha''<<<(x+y+1) \bmod 2]\neq 0$$

和

$$[\alpha'<<<y]\oplus[\alpha''<<<(x+y)]\oplus[\alpha''<<<((x+y+1) \bmod 2+2)]\neq 0.$$

故对 $W(\alpha)=3$,均有 $W(\alpha)+W(T_1\alpha)\geqslant 5$ 和 $W(\alpha)+W(T_2\alpha)\geqslant 5$.

(2.4) $W(\alpha)\geqslant 4$.

此时,由于 T_1, T_2 可逆,故 $T_1\alpha\neq 0, T_2\alpha\neq 0$,因此有 $W(\alpha)+W(T_1\alpha)\geqslant 5$ 和 $W(\alpha)+W(T_2\alpha)\geqslant 5$.故 T_1, T_2 的差分分支数均为 5.

(3) 证明 T_1 和 T_2 的差分分支数与线性分支数相等.

因 $M^T=Circ^R(a,b,c,d)$,且

$$T_1^T=\begin{pmatrix} M^T & (M>>>y)^T \\ (M>>>x)^T & [M>>>(x+y)]^T\oplus[M>>>((x+y+1)\bmod 2)]^T \end{pmatrix}$$
$$=\begin{pmatrix} M^T & M^T>>>y \\ M^T>>>x & [M^T>>>(x+y)]\oplus[M^T>>>((x+y+1)\bmod 2)] \end{pmatrix}.$$

类似地,有

$$T_2^T=\begin{pmatrix} M^T & M^T>>>y \\ M^T>>>x & [M^T>>>((x+y)\bmod 4)]\oplus[M^T>>>((x+y+1)\bmod 2+2)] \end{pmatrix}.$$

由第 2 步可知,T_1^T 与 T_2^T 的差分分支数为 5,即 T_1 和 T_2 的线性分支数为 5.

综上所述,T_1 和 T_2 是可逆且差分、线性分支数等于 5 的 0-1 矩阵. □

引理 1[9]. 设 A 是 $GF(2^n)$上的 $n\times n$ 矩阵,若交换矩阵 A 的行或列,则 A 的差分分支数与线性分支数保持不变.若 A^T 可由若干次交换矩阵 A 的行或列得到,则 A 的差分分支数与线性分支数相等.

备注 1. E2 算法采用的二元扩散矩阵可由定理 2 直接得到;Camellia 算法中的二元扩散矩阵可由定理 2 得出的矩阵通过交换行列得到.

备注 2. 不考虑交换行列,定理 2 一共可以构造出 64 个分支数达到 5 的 8 阶二元矩阵.

3 一类差分分支数与线性分支数相等的矩阵构造方法

定义 2. 若 n 阶方阵 $A=(a_{i,j})_{n\times n}$ 满足 $a_{i,j}=a_{0,(j-i)\bmod n}$,则 A 称为右循环移位方阵,记作 $A=Circ^R(a_{0,0},a_{0,1},\ldots,a_{0,n-1})$;

若 n 阶方阵 $B=(b_{i,j})_{n\times n}$ 满足 $b_{i,j}=b_{0,(i+j)\bmod n}$,则 B 称为左循环移位方阵,记作 $B=Circ^L(b_{0,0},b_{0,1},\ldots,b_{0,n-1})$;若 mn 阶方阵 $M=(M_{i,j})_{n\times n}$ 满足 $M_{i,j}=M_{0,(j-i)\bmod n}$,则将 M 称为右块循环移位方阵,记作 $M=Circ^R(M_{0,0},M_{0,1},\ldots,M_{0,n-1})$;若 mn 阶方阵 $N=(N_{i,j})_{n\times n}$ 满足 $N_{i,j}=N_{0,(i+j)\bmod n}$,则将 N 称为左块循环移位方阵,记作 $N=Circ^L(N_{0,0},N_{0,1},\ldots,N_{0,n-1})$.这里的 $M_{i,j}$ 与 $N_{i,j}$ 均为 m 阶方阵.

引理 2. 设双射 $\pi:\{0,1,\ldots,m-1\}\to\{0,1,\ldots,m-1\}$,$T=(t_{i,j})_{m\times m}$ 为 $GF(2^n)$上的矩阵且

$$t_{i,j}=\begin{cases}1, & j=\pi(i)\\ 0, & \text{其他}\end{cases},$$

则$\forall A=(a_{i,j})_{m\times m}$,有 $T\cdot A=(\alpha_{\pi(0)}^T,\alpha_{\pi(1)}^T,\ldots,\alpha_{\pi(m-1)}^T)^T$ 和 $A\cdot T=(\beta_{\pi(0)},\beta_{\pi(1)},\ldots,\beta_{\pi(m-1)})$.这里,

$$\alpha_i=(a_{i,0},a_{i,1},\ldots,a_{i,m-1}),\beta_i=(a_{0,i},a_{1,i},\ldots,a_{m-1,i})^T.$$

证明:设 $A=(a_{i,j})$,令 $L=T\cdot A=(l_{i,j})$,$R=A\cdot T=(r_{i,j})$,则

$$l_{i,j}=\bigoplus_{k=0}^{m-1}t_{i,k}a_{k,j}=t_{i,\pi(i)}a_{\pi(i),j}=a_{\pi(i),j},r_{i,j}=\bigoplus_{k=0}^{m-1}a_{i,k}t_{k,j}=a_{i,\pi(i)}t_{\pi(i),j}=a_{i,\pi(i)}.$$

故有$(l_{i,0},l_{i,1},\ldots,l_{i,m-1})=(a_{\pi(i),0},a_{\pi(i),1},\ldots,a_{\pi(i),m-1})$和$(r_{i,0},r_{i,1},\ldots,r_{i,m-1})=(a_{0,\pi(i)},a_{1,\pi(i)},\ldots,a_{m-1,\pi(i)})^T$. □

引理 3. 设 $A_0,A_1,\ldots,A_{l-1}$ 均为 $GF(2^n)$上的 $m\times m$ 矩阵,则 $A=CIRC^R(A_0,A_1,\ldots,A_{l-1})$与 $A'=CIRC^R(A_0,A_{l-1},\ldots,A_1)$的差分分支数与线性分支数相同.

证明:令 $lm\times lm$ 矩阵 $Q=CIRC^L(E,O,\ldots,O)$,这里的 E 表示 m 阶单位矩阵,O 表示 m 阶 0 矩阵.则 $A=QA'Q$.Q 是每行每列中有且仅有一个 1 元素的 0-1 矩阵.故由引理 2 知,A 可由矩阵 A'交换行列得到.再由引理 1 的结论可知,本定理结论成立. □

备注 3. 特别指出,当 $m=1$ 时有 $A'=A^T$ 成立.此时,引理 3 的结论退化为:循环移位矩阵的差分分支数和线性分支数相等[10].

更进一步地,可给出一类差分分支数与线性分支数相等的矩阵.

定理 3. 设 $A_0,A_1,\ldots,A_{l-1}$ 为 $GF(2^n)$上的 $n\times n$ 右循环方阵,则 $A=CIRC^R(A_0,A_1,\ldots,A_{l-1})$的差分分支数与线性分支数相同.

证明:令 $n\times n$ 矩阵 $P=Circ^L(1,0,\ldots,0)$,则类似引理 3 的证明过程知$\forall X=Circ^R(x_0,x_1,\ldots,x_{n-1})$,均有 $X^T=PXP$.设 E 为示 n 阶单位矩阵,O 为 n 阶 0 矩阵, $B=CIRC^R(A_0^T,A_1^T,\ldots,A_{l-1}^T)$,则

$$\begin{aligned}B&=CIRC^R(P,O,\ldots,O)\cdot CIRC^R(A_0,A_1,\ldots,A_{l-1})\cdot CIRC^R(P,O,\ldots,O)\\&=CIRC^R(P,O,\ldots,O)\cdot A\cdot CIRC^R(P,O,\ldots,O).\end{aligned}$$

注意到 $CIRC^R(P,O,\ldots,O)$是每行每列中有且仅有一个 1 元素的 0-1 矩阵,故由引理 2 知,B 可以通过 A 交换行列得到.根据引理 1 知,B 与 A 的差分分支数相同.

另一方面, $A^T=CIRC^R(A_0^T,A_{l-1}^T,\ldots,A_1^T)$,则由引理 3 知,$B$ 与 A^T 的差分分支数相同.即 A 与 A^T 的差分分支数相同.由定义 1,A 的差分分支数与线性分支数相同. □

文献[8]指出,16 阶 0-1 矩阵分支数最大为 8.本文计算了 10^8 个随机给出的 16 阶可逆 0-1 矩阵的分支数,未能找出分支数为 8 的矩阵;同时,本文验证了满足定理 3 条件的全部 2^{16} 个 16 阶 0-1 矩阵,其中,9 216 个矩阵的分支数达到 8 且 1 536 个同时满足对合性.实验说明,具有定理 3 的结构的 0-1 矩阵分支数达到最大的概率比随机选取的 0-1 矩阵大得多,因而是构造二元矩阵的一种实用方法.

4 结束语

扩散结构是密码设计的内容之一.利用 $GF(2^n)$上的 0-1 矩阵来设计扩散结构是当前分组密码扩散结构设计的一种重要思路.本文证明了有限域上 $GF(2^n)$的矩阵分支数就是该矩阵在扩域 $GF(2^{mn})$上的分支数,从而为扩散结构的分支数分析及大分支数扩散结构的构造带来了便利.基于该结论,本文补充了 Choy 等人关于二元矩阵分支数上界的证明.我们还给出了分支数达到 5 的 8 阶可逆 0-1 矩阵的一种构造方法,构造了一类差分分支数和线性分支数相等的矩阵,并从中搜索出了大量分支数为 8 的 16 阶可逆二元矩阵和二元对合矩阵.与随机搜索相比,

本文给出结构的实现效率要高得多.本文的研究结果为实际应用中 8 阶与 16 阶二元矩阵的构造提供了一种新的途径.

References:

[1] Daemen J, Rijmen V. The wide trail design strategy. In: Honary B, ed. Proc. of the Cryptography and Coding 2001. Springer-Verlag, 2001. 222−238. [doi: 10.1007/3-540-45325-3_20]

[2] Xiao L, Heys H. Hardware design and analysis of block cipher components. In: Lee PJ, ed. Proc. of the ICISC 2002. Seoul: Springer-Verlag, 2003. 164−181.

[3] Aoki K, Ichikawa T, Kanda M, Matsui M, Moriai S, Nakajima J, Tokita T. Camellia: A 128-bit block cipher suitable for multiple platforms—Design and analysis. In: Stinson DR, Tavares SE, eds. Proc. of the Selected Areas in Cryptography 2000. Waterloo: Springer-Verlag, 2000. 39−56. [doi: 10.1007/3-540-44983-3_4]

[4] NTT-Nippon Telegraph and Telephone Corporation. E2-a 128-bit block cipher. 2007. http://info.isl.ntt.co.jp/e2

[5] Kwon D, Kim J, Park S, Sung SH, Sohn Y, Song JH, Yeom Y, Yoon EJ, Lee S, Lee J, Chee S, Han D, Hong J. New block cipher: ARIA. In: Lim JI, Lee DH, eds. Proc. of the ICICS 2003. Seoul: Springer- Verlag, 2003. 432−445. [doi: 10.1007/978-3-540-24691-6_32]

[6] Choy JL, Khoo KM. New applications of differential bounds of the SDS structure. Report, 2008/395, Cryptology ePrint Archive, 2008. [doi: 10.1007/978-3-540-85886-7_26]

[7] Shao ZY, Wang H. Construction method for binary matrix with maximum branch number. Computer Engineering and applications, 2008,44(35):103−118 (in Chinese with English abstract).

[8] Koo BW, Jang HS, Song JH. Constructing and cryptanalysis of a 16×16 binary matrix as a diffusion layer. In: Chae K, Yung M, eds. Proc. of the WISA 2003. Jeju Island: Springer-Verlag, 2003. 489−503. [doi: 10.1007/978-3-540-24591-9_36]

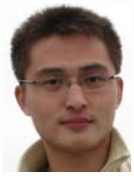
[9] Kang J, Hong S, Lee S, Yi O, Park C, Lim J. Practical and provable security against differential and linear cryptanalysis for substitution- permutation networks. ETRI Journal, 2001,23(4):158−167. [doi: 10.4218/etrij.01.0101.0402]

[10] Wu WL, Feng DG, Zhang WT. The Design and Analysis of Block Cipher. 2nd ed., Beijing: Tsinghua University Press, 2009. 237 (in Chinese).

附中文参考文献:

[7] 邵增玉,王洪.二元最佳扩散矩阵的一种构造方法.计算机工程与应用,2008,44(35):103−118.

[10] 吴文玲,冯登国,张文涛.分组密码的设计与分析.第 2 版,北京:清华大学出版社,2009.237.



崔霆(1985－),男,安徽铜陵人,博士生,主要研究领域为分组密码.

金晨辉(1965－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.

陈河山(1973－),男,讲师,主要研究领域为微分方程及其应用.