分组密码 Cauchy 型 MDS 扩散结构的几点注记

崔 霆,金晨辉
(信息工程大学电子技术学院,河南郑州 450004)

摘 要: MDS 矩阵是设计分组密码扩散结构的一种重要手段,由有序数组生成的 Cauchy 矩阵是一类基本的 MDS 矩阵.本文给出了两个有序数组生成的 Cauchy 矩阵相同的充要条件,证明了有限域上 Cauchy 矩阵的个数,证明了 Cauchy 矩阵一定不是循环移位矩阵;给出了 Cauchy 矩阵的不同元素个数达到最小值的充要条件,给出了使不同元素个数达到最少,同时 1 的个数达到最多的 Cauchy 矩阵的构造方法.此外,本文还提出了对合 Cauchy 矩阵的一种构造方法.

关键词: 分组密码; 扩散结构; MDS (Maximum Distance Separable) 矩阵; Cauchy 矩阵; 对合矩阵
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 07-1603-05

Several Remarks of Cauchy Type MDS Diffusion Layer for Block Cipher

CUI Ting, JIN Chen-hui
(*Institution of Electronic Technology, Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: Designing MDS matrices is one of the most important methods to construct diffusion layer for block ciphers, and Cauchy matrices generated by ordered-array is a basic kind of MDS matrices. This paper provides the necessary and sufficient condition of two distinct ordered-arrays generating one same Cauchy matrix. We show the count value of Cauchy matrices over finite field, and predicate that a Cauchy matrix could never be a cyclic-shift matrix. Further, this paper provides the necessary and sufficient condition of Cauchy matrices with minimum number of entries, and supplies the construct method of Cauchy matrix with minimum number of entries and maximum number of occurrences of 1. Additionally, this paper provides a construction for involution Cauchy matrices.

Key words: block cipher; diffusion layer; MDS (maximum distance separable) matrices; Cauchy matrices; involution matrices

1 引言

扩散结构的选择对分组密码的安全性和实现效率有着重要的影响[1~3].与扩散结构的其他设计方法相比,采用 MDS 矩阵设计的扩散结构可以最大限度地保证许多分组密码模型在差分和线性意义下的安全性,因此利用 MDS 矩阵设计扩散结构是一种常见的设计途径[4~6].在 AES、TWOFISH、Anubis 等密码算法中,设计者均使用 MDS 矩阵设计扩散结构.当矩阵的级数较小时,通过对随机矩阵检测的方法就能从中挑选出 MDS 矩阵,但是当矩阵的级数较大时这种方法将会失效,此时就需要寻找构造 MDS 矩阵的数学方法.由于 Cauchy 矩阵[5]一定是 MDS 矩阵,且 Cauchy 矩阵的级数可以任意大,因而将 MDS 矩阵设计为 Cauchy 矩阵是构造分组密码扩散结构的一种有效方法[5].

有限域 $GF(2^n)$ 上的 m 级 Cauchy 矩阵是基于 $GF(2^n)$ 上的一个元素互不相同的有序数组 $(x_0, x_1, \cdots, x_{2m-1})$ 构造的[7].在 Cauchy 矩阵的应用中,还有许多重要问题需要解决:两个不同的有序数组是否会产生相同的 Cauchy 矩阵? Cauchy 矩阵的数量是否足够多,能否提供足够多的 MDS 矩阵供设计者挑选? 此外,在密码算法的实现中,还希望 MDS 矩阵中不同元素的个数尽量地少,同时 1 元素的个数尽量地多,甚至希望 MDS 矩阵是对合矩阵,从而简化 MDS 矩阵的逆矩阵的实现,节省加脱密算法的实现开销.

对于上述问题,除文献[7,8]给出了一类对合 Cauchy 矩阵的构造方法外,其他问题都没有解决.

本文将研究上述问题.我们将首先给出两个有序数组生成同一个 Cauchy 矩阵的充要条件,进而给出 Cauchy

收稿日期:2010-02-08;修回日期:2010-06-07
基金项目:河南省杰出青年科学基金(No.0312001800)

矩阵的计数公式;接着我们将给出使不同元素个数最少且 1 元素个数最多的 Cauchy 矩阵的构造方法;最后本文将给出对合 Cauchy 矩阵的一种更加一般的构造方法,由于文献[7]提出的对合 Cauchy 矩阵的构造方法是该方法的特例,因而该方法将能构造出更多的对合 Cauchy 矩阵.此外,我们还将证明 Cauchy 矩阵一定不是循环移位矩阵.

2 预备知识

约定:$\oplus$表示逐位模 2 加,+ 表示实数加,a^{-1}表示有限域 $GF(2^n)$中元素 a 的乘法逆元,# ·表示集合中元素个数.$\boldsymbol{M}^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{M}$ 的转置.对 $\boldsymbol{y}=(y_1,y_2,\cdots,y_m)\in[GF(2^n)]^m$,用 $W(\boldsymbol{y})$表示 $y_1,y_2,\cdots,y_m$ 中非 0 元的个数,用 $\varnothing$ 表示空集.

首先介绍线性变换的差分分支数和线性分支数的定义.

定义 1[9] 设 $f(x)=\boldsymbol{A}x$,$\boldsymbol{A}$ 是 $GF(2^n)$上的 $m\times m$ 矩阵,$\boldsymbol{x}$ 为 $GF(2^n)$上的 m 维列向量,则分别称

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

和

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

为 f 的差分分支数和线性分支数.

众所周知,对于由 $GF(2^n)$上 $m\times m$ 矩阵 $\boldsymbol{A}$ 定义的线性变换 $f(x)=\boldsymbol{A}x$,其差分分支数达到最大值 $m+1$ 等价于其线性分支数达到最大值 $m+1$.当 $\boldsymbol{A}$ 的差分分支数达到最大值时,称 $\boldsymbol{A}$ 为 MDS 矩阵.文献[7]指出,$GF(2^n)$上的 Cauchy 矩阵都是 MDS 矩阵.下面给出 Cauchy 矩阵的定义.

定义 2[7] 设 $x_0,x_1,\cdots,x_{2m-1}$是 $GF(2^n)$中的互异元,对 $0\leqslant i,j\leqslant m-1$,令 $a_{i,j}=(x_i\oplus x_{m+j})^{-1}$,则称矩阵 $(a_{i,j})_{m\times m}$为有限域 $GF(2^n)$上由有序数组$(x_0,x_1,\cdots,x_{2m-1})$生成的 Cauchy 矩阵.

3 Cauchy 型 MDS 矩阵的计数

不同的有序数组可能会生成同一个 Cauchy 矩阵,对此有下面的定理.

定理 1 设 $\boldsymbol{C}=(c_{i,j})_{m\times m}$是 $GF(2^n)$上有序数组 $\boldsymbol{X}=(x_0,\cdots,x_{2m-1})$生成的 Cauchy 矩阵,$\boldsymbol{D}=(d_{i,j})_{m\times m}$是 $GF(2^n)$上有序数组 $\boldsymbol{Y}=(y_0,\cdots,y_{2m-1})$生成的 Cauchy 矩阵,则 $\boldsymbol{C}=\boldsymbol{D}$ 的充要条件为存在$\delta\in GF(2^n)$,使得对$\forall 0\leqslant k\leqslant 2m-1$,均有 $x_k=y_k\oplus\delta$.

证明 充分性.由定义 2,$\forall 0\leqslant i,j\leqslant m-1$,均有

$$\begin{aligned}c_{i,j}&=(x_i\oplus x_{m+j})^{-1}\\&=[(y_i\oplus\delta)\oplus(y_{m+j}\oplus\delta)]^{-1}\\&=(y_i\oplus y_{m+j})^{-1}=d_{i,j}\end{aligned}$$

故充分性成立.

必要性.$\boldsymbol{C}=\boldsymbol{D}$ 等价于$\forall 0\leqslant i,j\leqslant m-1$ 均有 $c_{i,j}=d_{i,j}$,即$(x_i\oplus x_{m+j})^{-1}=(y_i\oplus y_{m+j})^{-1}$,也即 $x_i\oplus y_i=x_{m+j}\oplus y_{m+j}$对$\forall 0\leqslant i,j\leqslant m-1$ 均成立.设 $x_0\oplus y_0=\delta$,则由 $x_i\oplus y_i=x_{m+j}\oplus y_{m+j}$知,对$\forall 0\leqslant k\leqslant 2m-1$,$x_k\oplus a_k=\delta$ 均成立. 证毕

推论 1 设 $\boldsymbol{A}$ 为 $GF(2^n)$上的 Cauchy 矩阵,则 $GF(2^n)$上能够生成 $\boldsymbol{A}$ 的有序数组恰有 2^n 个.

定理 2 $GF(2^n)$中有$A_{2^n}^{2^m}/2^n$ 个两两不同的 m 阶 Cauchy 矩阵.

证明 记有序数组集 $\Omega=\{\boldsymbol{X}:\boldsymbol{X}=(x_0,\cdots,x_{2m-1}),x_0,\cdots,x_{2m-1}\in GF(2^n)$且互异$\}$,则 $\#\Omega=A_{2^n}^{2^m}$.再由定理 1 和推论 1 知,$GF(2^n)$中 Cauchy 矩阵的个数为 $\#\Omega/2^n=A_{2^n}^{2^m}/2^n$. 证毕

4 最简 Cauchy 型 MDS 矩阵的性质

算法如果需要高效实现,则要求 Cauchy 矩阵中元素"1"的个数尽量多以及不同元素个数尽量少.本节将根据这两个标准对 Cauchy 矩阵进行研究.

定理 3 Cauchy 矩阵的任一行任一列中没有相同元素.

证明 仅对行的情形加以证明.设 $\boldsymbol{A}=(a_{i,j})_{m\times m}$为 $GF(2^n)$上有序数组 $\boldsymbol{X}=(x_0,\cdots,x_{2m-1})$生成的 Cauchy 矩阵.若存在 $0\leqslant s,k\leqslant m-1$,使得 $a_{t,s}=a_{t,k}$,则$(x_t\oplus x_{m+s})^{-1}=(x_t\oplus x_{m+k})^{-1}$,因而 $x_{m+s}=x_{m+k}$,这与 Cauchy 矩阵的定义矛盾.同样可以证明列的情形. 证毕

由定理 3 知 m 阶 Cauchy 矩阵的不同元素个数不少于 m.需要指出,不同元素个数恰为 m 的 m 阶 Cauchy 矩阵是存在的.以下讨论不同元素个数达到 m 的 m 阶 Cauchy 矩阵的结构.

定义 3 若 m 阶 Cauchy 矩阵的不同元素个数恰等于 m,则称该 Cauchy 矩阵为最简 Cauchy 矩阵.

由定义 3 和定理 3 知,m 阶最简 Cauchy 矩阵中每个元素出现的次数恰为 m.

定义 4[10] 设 X,Y,Z 均为具有 n 个点的有限集,$f:\boldsymbol{X}\times\boldsymbol{Y}\to\boldsymbol{Z}$,若对$\forall x_0\in\boldsymbol{X}$,$\forall y_0\in\boldsymbol{Y}$,以 y 为变量的映射$f(x_0,y)$是 $\boldsymbol{Y}$ 至 $\boldsymbol{Z}$ 的双射,且以 x 为变量的映射$f(x,y_0)$是 $\boldsymbol{X}$ 至 $\boldsymbol{Z}$ 的双射,则称 f 为拉丁方变换.

定理 4 给出了最简 Cauchy 矩阵的充要条件.

定理 4 $GF(2^n)$上的矩阵 $\boldsymbol{A}=(a_{i,j})_{m\times m}$为最简 Cauchy 矩阵的充要条件为 $a_{0,0},a_{0,1},\cdots,a_{0,m-1}$两两不同,且存在 $Z_m\times Z_m\to Z_m$ 的拉丁方变换f,使对$\forall i,j,k$,都有 $a_{i,j}=a_{0,f(i,j)}$和 $a_{0,f(i,j)}^{-1}\oplus a_{0,j}^{-1}=a_{0,f(i,k)}^{-1}\oplus a_{0,k}^{-1}$.

证明 必要性.设 $GF(2^n)$上的矩阵 $\boldsymbol{A}=(a_{i,j})_{m\times m}$

为最简 Cauchy 矩阵,则 $\boldsymbol{A}$ 中有且仅有 m 个不同元素.由定理 3 知,$a_{0,0}, a_{0,1}, \cdots, a_{0,m-1}$两两不同,因而是 $\boldsymbol{A}$ 的全部不同元,故对 $\forall 0 \leqslant i,j \leqslant m-1$, $a_{i,j}$必为 $a_{0,0}, a_{0,1}, \cdots, a_{0,m-1}$其中之一.构造变换 $f: Z_m \times Z_m \to Z_m$,使得对 $\forall 0 \leqslant i,j \leqslant m-1$ 都有 $a_{i,j} = a_{0,f(i,j)}$.由 $a_{0,f(i,j)} = a_{i,j}$以及 $\boldsymbol{A}$ 的每行每列元素互不相同知,f 为 $Z_m \times Z_m \to Z_m$ 的拉丁方变换.再设 $\boldsymbol{A} = (a_{i,j})_{m\times m}$由有序数组 $\boldsymbol{X} = (x_0, \cdots, x_{2m-1})$生成,则 $\forall i,j,k$ 均有 $a_{0,f(i,j)}^{-1} \oplus a_{0,j}^{-1} = x_i \oplus x_{m+j} \oplus x_0 \oplus x_{m+j} = x_i \oplus x_{m+k} \oplus x_0 \oplus x_{m+k} = a_{0,f(i,k)}^{-1} \oplus a_{0,k}^{-1}$,故必要性成立.

充分性.由于 $a_{0,0}, a_{0,1}, \cdots, a_{0,m-1}$两两不同,且对 $\forall i,j$ 有 $a_{i,j} = a_{0,f(i,j)}$,则 $\boldsymbol{A}$ 中不同元素个数为 m.令有序数组 $\boldsymbol{X} = (0, a_{0,f(1,0)}^{-1} \oplus a_{0,0}^{-1}, \cdots, a_{0,f(m-1,0)}^{-1} \oplus a_{0,0}^{-1}, a_{0,0}^{-1}, \cdots, a_{0,m-1}^{-1})$,由 $a_{0,0}, a_{0,1}, \cdots, a_{0,m-1}$两两不同知,数组 $\boldsymbol{X}$ 的后 m 个分量两两不等.对 $0 \leqslant i \neq j \leqslant m-1$,由 f 是拉丁方变换知 $a_{0,f(i,0)}^{-1} \neq a_{0,f(j,0)}^{-1}$,故 $a_{0,f(i,0)}^{-1} \oplus a_{0,0}^{-1} \neq a_{0,f(j,0)}^{-1} \oplus a_{0,0}^{-1}$,即 $0 \leqslant i \neq j \leqslant m-1$ 时,$\boldsymbol{X}$ 的第 i 个分量与第 j 个分量不等.根据条件又知 $a_{0,f(i,0)}^{-1} \oplus a_{0,0}^{-1} = a_{0,f(i,j)}^{-1} \oplus a_{0,j}^{-1} \neq a_{0,j}^{-1}$,故 $\boldsymbol{X}$ 中无重复分量.由 $(a_{0,f(i,0)}^{-1} \oplus a_{0,0}^{-1} \oplus a_{0,j}^{-1})^{-1} = (a_{0,f(i,j)}^{-1} \oplus a_{0,j}^{-1} \oplus a_{0,j}^{-1})^{-1} = a_{0,f(i,j)} = a_{i,j}$知,$\boldsymbol{A}$ 是有序数组 $\boldsymbol{X}$ 生成的 Cauchy 矩阵,也即 $\boldsymbol{A}$ 是最简 Cauchy 矩阵,充分性成立.　　证毕

推论 2　设 $\boldsymbol{A} = (a_{i,j})_{m\times m}$为 $GF(2^n)$ 上的最简 Cauchy 矩阵,f 为 $Z_m \times Z_m \to Z_m$ 的拉丁方变换,若 $\forall i,j$ 都有 $a_{i,j} = a_{0,f(i,j)}$,则 $f(i,f(i,j)) = j$.

证明　设 $\boldsymbol{A} = (a_{i,j})_{m\times m}$为有序数组 $\boldsymbol{X} = (x_0, \cdots, x_{2m-1})$生成的 Cauchy 矩阵,由 $a_{i,j} = a_{0,f(i,j)}$和 $a_{i,f(i,j)} = a_{0,f(i,f(i,j))}$知 $x_{m+f(i,j)} = x_i \oplus x_{m+j} \oplus x_0$ 和 $x_{m+f(i,j)} = x_i \oplus x_0 \oplus x_{m+f(i,f(i,j))}$成立,即 $f(i,f(i,j)) = j$.　　证毕

推论 3　设 $m > 2$, k 是自然数,矩阵 $\boldsymbol{B} = (b_{i,j})_{m\times m}$, $b_{i,j} = b_{0,(i+kj) \bmod m}$,则 $\boldsymbol{B}$ 不可能是 Cauchy 矩阵.

证明　若矩阵 $\boldsymbol{B}$ 构成 Cauchy 矩阵,由 $\boldsymbol{B}$ 中只包含 m 个元素,其必为最简 Cauchy 矩阵.由 $b_{i,j} = b_{0,(i+kj) \bmod m}$知,定理 4 中的拉丁方变换为 $f(i,j) = (i+kj) \bmod m$,故根据推论 2,$\forall i,j$ 都有

$$\begin{aligned} f(i,f(i,j)) &= (i + k(i+kj) \bmod m) \bmod m \\ &= [(k+1)i + k^2 j] \bmod m = j. \end{aligned}$$

取 $i=0, j=2$ 时,有 $2k^2 \bmod m = 1$,即 $m \mid (2k^2-1)$;取 $i=2, j=0$ 时,则有 $2(k+1) \bmod m = 0$,即 $m \mid (2k+2)$.注意到 $2k^2 - 1 = 2(k+1)(k-1) + 1$,故 $m \mid \gcd(2k^2-1, 2k+2) = 1$,这与 $m > 2$ 的题设矛盾,故 $f(i,j)$不满足 $f(i, f(i,j)) = j$.这说明 $\boldsymbol{B}$ 不可能是 Cauchy 矩阵.　　证毕

推论 3 指出,当 $m > 2$ 时,Cauchy 矩阵一定不是循环移位矩阵.

最简 Cauchy 矩阵中未必包含 1 元素,下面提出一种对最简 Cauchy 矩阵改造的方法,使得改造后的 m 阶最简 Cauchy 矩阵中 1 元素的个数达到最大值 m.

定义 5[8]　设 $\boldsymbol{A} = (a_{i,j})$, $\boldsymbol{B} = (b_{i,j})$都是 $GF(2^n)$上 $m \times m$ 矩阵,如果存在 $h_1, h_2, \cdots, h_m \in GF(2^n) \setminus \{0\}$,使得对 $\forall 0 \leqslant i,j \leqslant m-1$,均有 $b_{i,j} = a_{i,j} h_j$,则称矩阵 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 等效.

定理 5[8]　若 $GF(2^n)$上的两个矩阵等效,则其具有相同的差分分支数和线性分支数.

定义 6　若 m 阶最简 Cauchy 矩阵中包含 1 元素,则称该矩阵为优化最简 Cauchy 矩阵.

显然 m 阶优化最简 Cauchy 矩阵中的 1 元素个数恰为 m.

定理 6　$GF(2^n)$上任何一个 m 阶最简 Cauchy 矩阵均等效于 m 个优化最简 Cauchy 矩阵.

证明　设 $\boldsymbol{A} = (a_{i,j})_{m\times m}$是 $GF(2^n)$上有序数组 $\boldsymbol{X} = (x_0, \cdots, x_{2m-1})$生成的最简 Cauchy 矩阵.对任意取定的 $k \in \{0,1,\cdots,m-1\}$,令 $\boldsymbol{A}_k = a_{0,k}^{-1} \boldsymbol{A}$,容易验证 $\boldsymbol{A}_k$ 是有序数组 $\boldsymbol{X}_k = (a_{0,k}x_0, \cdots, a_{0,k}x_{2m-1})$生成的 Cauchy 矩阵;由定义 3,$\boldsymbol{A}$ 中不同元素个数为 m,故 $a_{0,k}^{-1}\boldsymbol{A}$ 中不同元素个数也为 m,即 $\boldsymbol{A}_k$ 是最简 Cauchy 矩阵;注意到 $\boldsymbol{A}_k = a_{0,k}^{-1}\boldsymbol{A}$ 的第 0 行,第 k 列的元素恰为 1,故 $\boldsymbol{A}_k$ 为优化最简 Cauchy 矩阵.　　证毕

定理 6 说明,可改造最简 Cauchy 矩阵,使得 1 元素的个数达到最大值 m.由于任一个最简 Cauchy 矩阵都与 m 个优化最简 Cauchy 矩阵等效,且二者的性能相近,因而在分组密码的设计中,可以根据需要,挑选合适的优化最简 Cauchy 矩阵.

5　对合 Cauchy 型 MDS 矩阵的构造

为了保证密码算法加脱密一致,设计者常采用对合变换来设计算法的环节.本节研究对合型 Cauchy 矩阵的设计.

Youssef 等[7]曾构造了一类对合的 Cauchy 矩阵,下面给出更加一般的构造方法.

定义 7　设映射 f 的原象集与象集均为非空集合 Δ,则 $\forall x \in \Delta$,称序列 $(x, f(x), f^2(x), \cdots)$为 x 在 f 作用下的轨道,记 $orbit_f(x) = \{x, f(x), f^2(x), \cdots\}$为 x 在 f 作用下的轨道集.当 Δ 为有限集时,对 $orbit_f(x)$中的任一元 x',称其为轨道集 $orbit_f(x)$的代表元.

定理 7　设 m 为偶数,$\boldsymbol{A} = (a_{i,j})_{m\times m}$为 $GF(2^n)$上有序数组 $\boldsymbol{X} = (x_0, \cdots, x_{m-1}, x_0 \oplus \delta, \cdots, x_{m-1} \oplus \delta)$生成的 Cauchy 矩阵,若集合 $\{x_0, \cdots, x_{m-1}\}$对 $\oplus$ 运算封闭,则 $\boldsymbol{A}$ 一定和对合矩阵 $\mu\boldsymbol{A}$ 等效,这里 $\mu = [\bigoplus_{k=0}^{m-1} (x_k \oplus$

$\delta)^{-1}]^{-1}$.

证明 设 $\boldsymbol{A}^2=\boldsymbol{C}=(c_{i,j})_{m\times m}$,则 $c_{i,j}=\bigoplus_{k=0}^{m-1}[(x_i\oplus x_k\oplus\delta)(x_k\oplus x_j\oplus\delta)]^{-1}$.当 $i=j$ 时,有 $c_{i,i}=\bigoplus_{k=0}^{m-1}(x_i\oplus x_k\oplus\delta)^{-2}$.因 $x_0,\cdots,x_{m-1}$ 两两互异,故 $x_i\oplus x_0,\cdots,x_i\oplus x_{m-1}$ 两两互异;同时由 $\{x_0,\cdots,x_{m-1}\}$ 对 $\oplus$ 运算封闭知,集合 $\{x_i\oplus x_0,\cdots,x_i\oplus x_{m-1}\}$ 中的任一元均包含于 $\{x_0,\cdots,x_{m-1}\}$,故集合 $\{x_0,\cdots,x_{m-1}\}$ 与集合 $\{x_i\oplus x_0,\cdots,x_i\oplus x_{m-1}\}$ 相等,因而 $c_{i,i}=\bigoplus_{k=0}^{m-1}(x_i\oplus x_k\oplus\delta)^{-2}=\bigoplus_{k=0}^{m-1}(x_k\oplus\delta)^{-2}$.当 $i\neq j$ 时,构造映射 $g_{i,j}:Z_m\to Z_m$,使得对 $\forall 0\leqslant k\leqslant m-1$ 均成立 $x_{g_{i,j}(k)}=x_i\oplus x_j\oplus x_k$.由 $g_{i,j}$ 的定义,有 $g_{i,j}(g_{i,j}(k))=k$,同时由 $x_{g_{i,j}(k)}\oplus x_k=x_i\oplus x_j\neq 0$ 知 $x_{g_{i,j}(k)}\neq x_k$,即 $g_{i,j}(k)\neq k$,因而对 $\forall 0\leqslant k\leqslant m-1$ 均有 $orbit_{g_{i,j}}(k)=\{k,g_{i,j}(k)\}$.令集合 Λ 为所有不同轨道中各抽出一个代表元所组成的集合,则 $Z_m=\bigcup_{k\in\Lambda}orbit_{g_{i,j}}(k)$,且当 $k_1\neq k_2$ 时,$orbit_{g_{i,j}}(k_1)\cap orbit_{g_{i,j}}(k_2)=\varnothing$.故

$$\begin{aligned}c_{i,j}&=\bigoplus_{k=0}^{m-1}[(x_i\oplus x_k\oplus\delta)(x_k\oplus x_j\oplus\delta)]^{-1}\\&=\bigoplus_{k\in\Lambda}\Big[\bigoplus_{t\in orbit_{g_{i,j}}(k)}[(x_i\oplus x_t\oplus\delta)(x_t\oplus x_j\oplus\delta)]^{-1}\Big],\end{aligned}$$

又由 $g_{i,j}$ 定义知 $x_i\oplus x_k\oplus\delta=x_{g_{i,j}(k)}\oplus x_j\oplus\delta$ 和 $x_i\oplus x_{g_{i,j}(k)}\oplus\delta=x_k\oplus x_j\oplus\delta$ 成立,因此

$$\begin{aligned}&\bigoplus_{t\in orbit_{g_{i,j}}(k)}[(x_i\oplus x_t\oplus\delta)(x_t\oplus x_j\oplus\delta)]^{-1}\\&=[(x_i\oplus x_k\oplus\delta)(x_k\oplus x_j\oplus\delta)]^{-1}\\&\quad\oplus[(x_i\oplus x_{g_{i,j}(k)}\oplus\delta)(x_{g_{i,j}(k)}\oplus x_j\oplus\delta)]^{-1}\\&=0,\end{aligned}$$

故 $c_{i,j}=0$.即 $\boldsymbol{C}=\boldsymbol{A}^2=\bigoplus_{k=0}^{m-1}(x_k\oplus\delta)^{-2}\boldsymbol{E}$,这里 $\boldsymbol{E}$ 为 m 阶单位矩阵.同时由 $\boldsymbol{A}$ 是 Cauchy 矩阵,故 $\boldsymbol{A}$ 是 MDS 矩阵,因而 $\boldsymbol{A}$ 满秩,即 $\boldsymbol{A}^2$ 满秩,因此 $\bigoplus_{k=0}^{m-1}(x_k\oplus\delta)^{-2}\neq 0$.令 $\mu=[\bigoplus_{k=0}^{m-1}(x_k\oplus\delta)^{-1}]^{-1}$,则 $(\mu\boldsymbol{A})^2=\mu^2\boldsymbol{A}^2=\boldsymbol{E}$ 成立,即 $\boldsymbol{A}$ 和对合矩阵 $\mu\boldsymbol{A}$ 等效. 证毕

文献[7]中构造对合矩阵的方法是定理 7 的特例.

$\mu\boldsymbol{A}$ 是由有序数组 $\boldsymbol{X}'=(\mu^{-1}x_0,\cdots,\mu^{-1}x_{m-1},\mu^{-1}x_0\oplus\mu^{-1}\delta,\cdots,\mu^{-1}x_{m-1}\oplus\mu^{-1}\delta)$ 生成的 Cauchy 矩阵.

定理 7 提供了构造对合 MDS 矩阵的一种方法.

例如,在有限域 $GF(2)[x]/(x^4\oplus x\oplus 1)$ 中取 $x_0=10,x_1=2,x_2=8,x_3=0,\delta=3$,则有序数组 $\boldsymbol{X}=(10,2,8,0,9,1,11,3)$ 生成的 Cauchy 矩阵为

$$\boldsymbol{C}=\begin{bmatrix}14&5&1&2\\5&14&2&1\\1&2&14&5\\2&1&5&14\end{bmatrix},$$

$$\mu=[\bigoplus_{k=0}^{3}(x_k\oplus\delta)^{-1}]^{-1}=15,$$

由定理 7,矩阵 $\boldsymbol{C}_{Inv}=15\cdot\boldsymbol{C}=\begin{bmatrix}5&6&15&13\\6&5&13&15\\15&13&5&6\\13&15&6&5\end{bmatrix}$ 是对合最简 Cauchy 矩阵.

6 结束语

本文研究了 Cauchy 矩阵的部分性质,给出了两个有序数组生成同一个 Cauchy 矩阵的充要条件,并给出 Cauchy 矩阵的计数公式;接着我们给出了使不同元素个数最少且 1 元素个数最多的 Cauchy 矩阵的构造方法;最后本文给出了对合 Cauchy 矩阵的一种构造方法,与文献[7]的构造方法相比,本文的构造方法更加具有一般性.此外,我们还将证明 Cauchy 矩阵一定不是循环移位矩阵.本文的研究结果在密码的设计中具有应用价值.

参考文献

[1] 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.

[2] Wang M Q. Differential Cryptanalysis of Present. Cryptology ePrint Archive[R/OL]. http://eprint.iacr.org/2007/408, 2007.

[3] Wu W L, Zhang W T, Feng D G. Impossible differential cryptanalysis of reduce round ARIA and Camellia[J]. Journal of Computer Science and Technology, 2007, 22(3): 449 – 456.

[4] P Junod, S Vaudenay. Perfect diffusion primitives for block ciphers building efficient MDS matrices[A]. Selected Areas in Cryptography 2004[C]. Waterloo: Springer-Verlay, 2004. 84 – 99.

[5] Shirai T, Shibutani K. On Feistel structures using a diffusion switching mechanism[A]. Robshaw Fast Software Encryption, 13th International Workshop, FSE 2006[C]. Graz: Springer-Verlag, 2006. 41 – 56.

[6] 王念平,金晨辉,余昭平.对合型列混合变换的研究[J].电子学报,2005,33(10):1917 – 1920.
Wang N P, Jin C H, Yu Z P. Research on involution-typed mixcolumn transform[J]. Acta Electronica Sinica, 2005, 33(10): 1917 – 1920. (in Chinese)

[7] A Youssef, S Mister, S Tavares. On the design of linear transformations for substitution permutation encryption networks[A]. C Adams Workshop on Selected Areas in Cryptography-SAC'97[C]. Ottawa: Springer-Verlag, 1997. 40 – 48.

[8] 崔霆,金晨辉.对合 Cauchy-Hadamard 型 MDS 矩阵的构造

[J].电子与信息学报,2010,32(2):500 – 503.
Cui T, Jin C H. Construction of involution cauchy-hadamard type MDS matrices[J]. Journal of Electronics & Information Technology, 2010, 32(2): 500-503. (in Chinese)
[9] J Daemen. Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis[D]. Leuven: K U Leuven, 1995.
[10] 金晨辉. 拉丁方变换的几个等价刻画[J]. 通信学报, 2003, 24(6): 129 – 132.
Jin C H. Equivalent characteristics for Latin square transformations[J]. Journal of China Institute of Communications, 2003, 24(6): 129 – 132. (in Chinese)

作者简介

崔　霆　男,1985 年 12 月出生于安徽铜陵. 现为解放军信息工程大学博士研究生,从事分组密码的相关研究.
E-mail: cuiting_1209@yahoo.com.cn

金晨辉　男,解放军信息工程大学教授、博士生导师. 1965 年 3 月出生于河南扶沟. 主要研究方向为密码学与信息安全.