对合 Cauchy-Hadamard 型 MDS 矩阵的构造

崔　霆　　金晨辉
(信息工程大学电子技术学院　郑州　450004)

摘　要：MDS 矩阵和对合 MDS 矩阵在分组密码中有广泛应用。该文将考察同时是 Hadamard 矩阵和 Cauchy 矩阵的那些 MDS 矩阵，给出了这类矩阵的结构、构造方法和个数，从而得到了 MDS 矩阵一种新的构造方法。该文还证明了 Cauchy-Hadamard 型 MDS 矩阵都等效于对合的 Cauchy-Hadamard 型 MDS 矩阵，并给出了由 Cauchy-Hadamard 型 MDS 矩阵构造对合的 Cauchy-Hadamard 型 MDS 矩阵的方法。

关键词：分组密码；扩散结构；分支数；MDS 矩阵；Cauchy-Hadamard 矩阵
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2010)02-0500-04
DOI: 10.3724/SP.J.1146.2009.00070

Construction of Involution Cauchy-Hadamard Type MDS Matrices

Cui Ting　　Jin Chen-hui
(*Institution of Electronic Technology*, *Information Engineering University*, *Zhengzhou*, 450004 *China*)

Abstract: MDS matrices and involution MDS matrices are widely used in block ciphers. This paper deals with those MDS matrices which are Hadamard matrices and Cauchy matrices simultaneously. Then the structure, the method of constructing and the count value of this kind of matrices are presented. By this, a new method for constructing MDS matrices is obtained. Additionally, this paper proves that a Cauchy-Hadamard type MDS matrix can be transformed into an involution Cauchy-Hadamard type MDS, and then proposes a new method to construct an involution Cauchy-Hadamard type MDS matrix from a Cauchy-Hadamard type MDS matrix.

Key words: Block cipher; Diffusion structure; Branch number; MDS(Maximum Distance Separable) matrices; Cauchy-Hadamard matrices

1　引言

扩散结构的设计是分组密码算法设计的一个重要组成部分，扩散结构设计的好坏直接影响着密码算法的安全性和效率[1–3]。为了度量 S-P (Substitution-Permutation)网络的扩散结构的扩散效果，Rijmen 提出差分分支数与线性分支数的概念[4]。同时指出，采用差分分支数和线性分支数较大的扩散结构可以使 SP 结构更好地抵抗差分攻击和线性攻击。由于 MDS 矩阵的差分分支数和线性分支数相等且达到最大[5]，故利用 MDS 矩阵设计分组密码的扩散结构是一种重要而常用的方法。目前，MDS 矩阵广泛应用于分组密码扩散结构的设计。AES 算法，Anubis 算法，Twofish 算法和 Shark 算法等都采用 MDS 矩阵设计扩散结构。此外，为了保证脱密结构与加密结构的一致性，MDS 矩阵最好是对合矩阵。因此，如何构造对合型 MDS 矩阵也一直是人们关心的问题。文献[6]提出可以分别从循环移位矩阵，Cauchy 矩阵以及 Hadamard 矩阵等特殊的矩阵中搜索出便于实现的 MDS 矩阵。文献[7]进一步指出，循环移位型 MDS 矩阵不可能是对合的。文献[8]与文献[9]中提出了利用 Cauchy 型矩阵设计 MDS 矩阵的思想和构造方法，但能构造出的 MDS 矩阵的个数不多，即当矩阵的级数给定时，这两种方法都只能构造出一个或少数几个 MDS 矩阵。

本文将考察同时是 Hadamard 矩阵和 Cauchy 矩阵的那些矩阵，给出了这类矩阵的结构、构造方法和个数，从而给出了 MDS 矩阵和对合 MDS 矩阵的一种新的构造方法。由于这类 MDS 矩阵和对合 MDS 矩阵的结构非常清晰，构造方法简单明了，因而更便于实际应用。

2　预备知识

本文均用 $\oplus$ 表示逐位模 2 加，用 $+$ 表示实数加，用 a^{-1} 表示有限域 $\mathrm{GF}(2^n)$ 中元素 a 的乘法逆元。对于 $\boldsymbol{y}=(y_1,y_2,\cdots,y_m)\in[\mathrm{GF}(2^n)]^m$，本文均用 $W(\boldsymbol{y})$ 表示 $y_1,y_2,\cdots,y_m$ 中非 0 元的个数。

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[4]　设 $f:[\mathrm{GF}(2^n)]^m\to[\mathrm{GF}(2^n)]^m$ 是有限域

2009-01-16 收到，2009-06-29 改回
河南省杰出青年科学基金(0312001800)资助课题
通信作者：崔霆　cuiting_1209@yahoo.com.cn

$\mathrm{GF}(2^n)$ 上的多输出线性映射，令

$$D_f=\min\{W(\boldsymbol{\alpha})+W(\boldsymbol{\beta}):p_f(\boldsymbol{\alpha}\to\boldsymbol{\beta})=1,\ \boldsymbol{\alpha},\boldsymbol{\beta}\in\mathrm{GF}(2^n),\boldsymbol{\alpha}\neq 0\}$$

$$L_f=\min\{W(\boldsymbol{\alpha})+W(\boldsymbol{\beta}):|\rho_f(\boldsymbol{\alpha}\to\boldsymbol{\beta})|=1,\ \boldsymbol{\alpha},\boldsymbol{\beta}\in\mathrm{GF}(2^n),\boldsymbol{\beta}\neq 0\}$$

则分别称 D_f 和 L_f 为 f 的差分分支数和线性分支数。其中

$$p_f(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{2^{nm}}/\#\{\boldsymbol{x}\in[\mathrm{GF}(2^n)]^m:\ f(\boldsymbol{x}\oplus\boldsymbol{\alpha})\oplus f(\boldsymbol{x})=\boldsymbol{\beta}\}$$

$$\rho_f(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{2^{nm}}\sum_{\boldsymbol{x}\in[\mathrm{GF}(2^n)]^m}(-1)^{\boldsymbol{\beta}\cdot f(\boldsymbol{x})\oplus\boldsymbol{\alpha}\cdot\boldsymbol{x}}$$

且 $\boldsymbol{\alpha}\cdot\boldsymbol{x}=\alpha_1x_1\oplus\cdots\oplus\alpha_mx_m$ 是有限域 $\mathrm{GF}(2^n)$ 上 m 维向量 $\boldsymbol{\alpha}$ 与 m 维向量 $\boldsymbol{x}$ 的点积。

众所周知，对于由 $\mathrm{GF}(2^n)$ 上 $m\times m$ 矩阵 $\boldsymbol{A}$ 定义的线性变换 $f(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}$，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 $m+1$。当其差分分支数达到最大值时，则称 $\boldsymbol{A}$ 为 MDS 矩阵。

引理 1[5]　设 $f(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}$，且 $\boldsymbol{A}$ 是 $\mathrm{GF}(2^n)$ 上的 $m\times m$ 矩阵，则有

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

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

定义 2[6]　设 $\boldsymbol{A}=(a_{i,j})_{2^m\times 2^m}$ 是 $\mathrm{GF}(2^n)$ 上的 $2^m\times 2^m$ 矩阵，如果当 $0\le i,j\le 2^m-1$ 时，均有 $a_{i,j}=a_{0,i\oplus j}$，则称 $\boldsymbol{A}$ 为有限域 $\mathrm{GF}(2^n)$ 上的一个 Hadamard 矩阵，并简记 $\boldsymbol{A}=\mathrm{Had}(a_{0,0},a_{0,1},\cdots,a_{0,2^m-1})$。

下面给出 Hadamard 矩阵的差分分支数与线性分支数的特性。

定理 1　有限域上的 Hadamard 矩阵的差分分支数与线性分支数相等。

证明　由 Hadamard 矩阵是对称矩阵和引理 1 即证。　　证毕

引理 2[7]　有限域 $\mathrm{GF}(2^n)$ 上的矩阵是 MDS 矩阵当且仅当它的任一子矩阵都是满秩矩阵。

定理 2　有限域 $\mathrm{GF}(2^n)$ 上 Hadamard 矩阵 $\mathrm{Had}(a_0,a_1,\cdots,a_{2^m-1})$ 是 MDS 矩阵的必要条件是 $a_0,a_1,\cdots,a_{2^m-1}$ 两两不等且都不为 0。

证明　设 $\mathrm{Had}(a_0,a_1,\cdots,a_{2^m-1})=(b_{i,j})_{2^m\times 2^m}$，$i\neq j$，则由引理 2 知

$$a_i^2-a_j^2=\begin{vmatrix}a_i & a_j\\ a_j & a_i\end{vmatrix}=\begin{vmatrix}b_{0,i} & b_{0,j}\\ b_{i\oplus j,i} & b_{i\oplus j,j}\end{vmatrix}\neq 0$$

因而 $a_i\neq a_j$。再由 MDS 矩阵的元素都是非零元即知 $a_0,a_1,\cdots,a_{2^m-1}$ 两两不等且都不为 0。　　证毕

3　Cauchy-Hadamard 型 MDS 矩阵的结构、构造和计数

定义 3[8]　设 $x_0,\cdots,x_{m-1},y_0,\cdots,y_{m-1}$ 是 $\mathrm{GF}(2^n)$ 中的互异元，对 $0\le i,j\le m-1$，令 $a_{i,j}=(x_i\oplus y_j)^{-1}$，则称矩阵 $(a_{i,j})_{m\times m}$ 为有限域 $\mathrm{GF}(2^n)$ 上由 $\boldsymbol{X}=(x_0,\cdots,x_{m-1})$ 和 $\boldsymbol{Y}=(y_0,\cdots,y_{m-1})$ 决定的 Cauchy 矩阵。

文献 8 证明了有限域 $\mathrm{GF}(2^n)$ 上的 Cauchy 矩阵都是 MDS 矩阵，因而也称 Cauchy 矩阵为 Cauchy 型 MDS 矩阵。下面给出 Cauchy-Hadamard 矩阵的定义。

定义 4　如果有限域 $\mathrm{GF}(2^n)$ 上的 $2^m\times 2^m$ 矩阵同时是 Hadamard 矩阵和 Cauchy 矩阵，则称该矩阵为 Cauchy-Hadamard 矩阵或 Cauchy-Hadamard 型 MDS 矩阵，简称为 C-H 矩阵。

定理 3　设 $x_0,\cdots,x_{2^m-1}\in\mathrm{GF}(2^n)$ 互不相同，则存在 $\boldsymbol{Y}\in[\mathrm{GF}(2^n)]^m$，使得由 $\boldsymbol{X}=(x_0,\cdots,x_{2^m-1})$ 和 $\boldsymbol{Y}$ 能够决定一个 C-H 矩阵的充要条件是 $x_i\oplus x_j=x_0\oplus x_{i\oplus j}$ 对 $0\le i,j<2^m$ 都成立，且存在 $\mathrm{GF}(2^n)$ 中非零元 δ，使得 $x_i\oplus x_0\neq\delta$ 对 $0\le i<2^m$ 都成立。

证明　必要性：设 $\boldsymbol{A}=(a_{i,j})_{2^m\times 2^m}$ 是由 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 决定的 C-H 矩阵，$0\le i,j<2^m$，令 $\delta=a_{0,0}^{-1}$。由 $\boldsymbol{A}$ 是 C-H 矩阵知 $a_{0,0}=a_{i,i}=(x_i\oplus y_i)^{-1}$，从而 $y_i=x_i\oplus a_{0,0}^{-1}=x_i\oplus\delta$。由 $x_i\neq y_0$ 和 $y_0=x_0\oplus\delta$ 知 $x_i\oplus x_0\neq\delta$，再由 $a_{i,j}=a_{0,i\oplus j}$ 以及 $a_{i,j}=(x_i\oplus y_j)^{-1}$ 和 $a_{0,i\oplus j}=(x_0\oplus y_{i\oplus j})^{-1}$ 知 $x_i\oplus y_j=x_0\oplus y_{i\oplus j}$，从而有 $x_i\oplus x_0=y_{i\oplus j}\oplus y_j=(x_{i\oplus j}\oplus\delta)\oplus(x_j\oplus\delta)=x_{i\oplus j}\oplus x_j$，这说明必要性成立。

充分性：设 $i\neq j$，则 $x_i\oplus x_j=x_0\oplus x_{i\oplus j}\neq 0$，故 $x_0,\cdots,x_{2^m-1}$ 是 $\mathrm{GF}(2^n)$ 中的不同元。令 $y_i=x_i\oplus\delta$，则 $y_0,\cdots,y_{2^m-1}$ 也互不相同。由于 $x_i\oplus y_j=x_i\oplus x_j\oplus\delta=x_{i\oplus j}\oplus x_0\oplus\delta\neq 0$，故 $x_0,\cdots,x_{2^m-1},y_0,\cdots,y_{2^m-1}$ 互不相同，因而由 $\boldsymbol{X}$ 和 $(y_0,\cdots,y_{2^m-1})$ 能够决定一个 Cauchy 矩阵 $(a_{i,j})_{2^m\times 2^m}$，其中 $a_{i,j}=(x_i\oplus y_j)^{-1}$。再由

$$a_{i,j}=(x_i\oplus y_j)^{-1}=(x_i\oplus x_j\oplus\delta)^{-1}=(x_0\oplus x_{i\oplus j}\oplus\delta)^{-1}=(x_0\oplus y_{i\oplus j})^{-1}=a_{0,i\oplus j}$$

即知 $(a_{i,j})_{2^m\times 2^m}$ 是 Hadamard 矩阵，因而是 C-H 矩阵。这说明充分性成立。　　证毕

定理 3 解决了利用有限域 $\mathrm{GF}(2^n)$ 中 2^m 个不同元 $x_0,\cdots,x_{2^m-1}$，通过构造 C-H 矩阵的方法构造 MDS 矩阵时，$x_0,\cdots,x_{2^m-1}$ 应当满足的条件，其证明给出了构造出的 C-H 矩阵的结构。定理 3 还说明，构造 C-H 矩阵，等价于构造 $\mathrm{GF}(2^n)$ 中满足 $x_i\oplus x_j=x_0\oplus x_{i\oplus j}$ 的不同元 $x_0,x_1,\cdots,x_{2^m-1}$，并从 $\mathrm{GF}(2^n)\setminus\{0,x_1\oplus x_0,\cdots,x_{2^m-1}\oplus x_0\}$ 选取一个元作为 δ。因此，

也称 C-H 矩阵为基于$(\delta,x_0,x_1,\cdots,x_{2^m-1})$构造的 C-H 矩阵。下面解决 C-H 矩阵的计数问题。

定理 4 设$\boldsymbol{A}=(a_{i,j})_{2^m\times 2^m}$和$\boldsymbol{B}=(b_{i,j})_{2^m\times 2^m}$分别是 GF$(2^n)$上基于$(\delta,x_0,x_1,\cdots,x_{2^m-1})$和$(\delta',z_0,z_1,\cdots,z_{2^m-1})$构造的 C-H 矩阵，则$\boldsymbol{A}=\boldsymbol{B}$的充要条件是$\delta=\delta'$且存在$\varepsilon\in$GF$(2^n)$，使得当$0\le i\le 2^m-1$时，都有$x_i\oplus z_i=\varepsilon$。

证明 由$a_{i,j}=(x_i\oplus x_j\oplus\delta)^{-1}=[(z_i\oplus\varepsilon)\oplus(z_j\oplus\varepsilon)\oplus\delta']^{-1}=(z_i\oplus z_j\oplus\delta')^{-1}=b_{i,j}$知充分性成立。下面证明必要性。由$a_{i,j}=(x_0\oplus x_{i\oplus j}\oplus\delta)^{-1}$知$a_{0,0}=\delta^{-1}$，同理可证$b_{0,0}=\delta'^{-1}$，故由$\boldsymbol{A}=\boldsymbol{B}$知$\delta=\delta'$。再设$x_0\oplus z_0=\varepsilon$且$0\le i\le 2^m-1$，则由$(x_0\oplus x_i\oplus\delta)^{-1}=a_{i,0}=b_{i,0}=(z_0\oplus z_i\oplus\delta')^{-1}$知$x_i\oplus\varepsilon=z_i$，即必要性成立。 证毕

定理 4 说明，基于$(\delta,x_0,x_1,\cdots,x_{2^m-1})$构造的 C-H 矩阵与基于$(\delta,0,x_1\oplus x_0,\cdots,x_{2^m-1}\oplus x_0)$构造的C-H矩阵相等，因而只需基于$(\delta,0,x_1\oplus x_0,\cdots,x_{2^m-1}\oplus x_0)$构造的 C-H 矩阵即可。

下面研究满足定理 3 且$x_0=0$的$x_0,x_1,\cdots,x_{2^m-1}$的构造问题。

记$f(i)=x_i$，则$x_i\oplus x_j=x_0\oplus x_{i\oplus j}$等价于$x_i\oplus x_j=x_{i\oplus j}$，因而等价于$f(i)\oplus f(j)=f(i\oplus j)$，故$X$满足定理 3 的条件等价于$f:\text{GF}(2^m)\to\text{GF}(2^n)$是线性单射，因而等价于$f(2^0),f(2^1),\cdots,f(2^{m-1})$在二元域上线性无关，且$f\left(\overset{2^m-1}{\underset{i=0}{\oplus}}a_i2^i\right)=\overset{2^m-1}{\underset{i=0}{\oplus}}a_if(2^i)$。这说明$f$由 GF$(2^n)$中线性无关元$f(2^0),f(2^1),\cdots,f(2^{m-1})$唯一确定，且不同的$f(2^0),f(2^1),\cdots,f(2^{m-1})$构造出不同的$f$。由于GF$(2^n)$中线性无关元$f(2^0),f(2^1),\cdots,f(2^{m-1})$在考虑顺序时共有$\prod_{i=1}^{m}(2^n-2^{i-1})$个，因而 GF$(2^m)$至 GF$(2^n)$的线性单射共有$\prod_{i=1}^{m}(2^n-2^{i-1})$个，这就是满足定理 3 条件且$x_0=0$的$x_0,x_1,\cdots,x_{2^m-1}$的个数。

定理 5 GF(2^n)上的2^m级 C-H 矩阵共有$(2^n-2^m)\prod_{i=1}^{m}(2^n-2^{i-1})$个。

证明 显然，在考虑顺序时，GF(2^n)上的m个线性无关元共有$\prod_{i=1}^{m}(2^n-2^{i-1})$个选择，且可取$x_0=0$。由于对给定的$(x_0,x_1,\cdots,x_{2^m-1})$，$\delta$共有$2^n-2^m$个选择，因而满足$x_0=0$的$(\delta,x_0,x_1,\cdots,x_{2^m-1})$共有$(2^n-2^m)\prod_{i=1}^{m}(2^n-2^{i-1})$个选择，故由定理 4 知，由它们共可构造出$(2^n-2^m)\prod_{i=1}^{m}(2^n-2^{i-1})$个不同的 C-H 矩阵。 证毕

根据上述结果，在构造 C-H 矩阵时，可采取以下步骤：

步骤1 构造出 GF(2^n)中 m 个线性无关元$x_{2^0},x_{2^1},\cdots,x_{2^{m-1}}$；

步骤2 取$x_0=0$；

步骤3 根据$x_{\sum_{i=0}^{2^m-1}a_i2^i}=\overset{2^m-1}{\underset{i=0}{\oplus}}a_ix_{2^i}$，计算出所有的$x_0,x_1,\cdots,x_{2^m-1}$。这里诸$a_i\in\{0,1\}$；

步骤4 从$\text{GF}(2^n)\setminus\{x_0,x_1,\cdots,x_{2^m-1}\}$中选出一个元作为$\delta$；

步骤5 对$0\le i,j<2^m$，令$a_{i,j}=(x_{i\oplus j}\oplus\delta)^{-1}$。则矩阵$\boldsymbol{A}=(a_{i,j})_{2^m\times 2^m}$就是一个 C-H 矩阵。其中步骤 1 可通过以下步骤完成：

首先从$\text{GF}(2^n)\setminus\{0\}$中选出一个元作为$x_{2^0}$，对于$0\le i<m$，如果$x_{2^0},x_{2^1},\cdots,x_{2^i}$已经选好，则从$\text{GF}(2^n)\setminus\text{span}\{x_{2^0},x_{2^1},\cdots,x_{2^i}\}$中选一个元作为$x_{2^{i+1}}$，由此可递归地构造出$x_{2^0},x_{2^1},\cdots,x_{2^{m-1}}$。这里 span$\{x_{2^0},x_{2^1},\cdots,x_{2^i}\}$是 GF$(2^n)$的包含$x_{2^0},x_{2^1},\cdots,x_{2^i}$最小子域。

4 对合的 Cauchy-Hadamard 型 MDS 矩阵的构造

以上解决了 C-H 矩阵的构造和计数问题，下面研究对合 C-H 矩阵的结构和构造问题。

定理 6[6] 设$\boldsymbol{A}=\text{Had}(a_0,a_1,\cdots,a_{2^m-1})$是GF$(2^n)$上的 Hadamard 矩阵，则$\boldsymbol{A}^2=\left(\overset{2^m-1}{\underset{i=0}{\oplus}}a_i^2\right)\boldsymbol{E}$是主对角线上的元素均是$\overset{2^m-1}{\underset{i=0}{\oplus}}a_i^2$的对角矩阵。

定理 6 说明，在构造对合 Hadamard 矩阵时，只需在选定$a_1,\cdots,a_{2^m-1}$后，再取a_0，使得$\overset{2^m-1}{\underset{i=0}{\oplus}}a_i^2=1$即可。但是，在基于$(\delta,x_0,x_1,\cdots,x_{2^m-1})$构造 C-H 矩阵时，由于$\overset{2^m-1}{\underset{i=0}{\oplus}}a_i^2=\overset{2^m-1}{\underset{i=0}{\oplus}}(x_0\oplus x_i\oplus\delta)^{-2}$，因而采取先构造$x_0,x_1,\cdots,x_{2^m-1}$再构造$\delta$的方法构造对合 C-H 矩阵是很难奏效的。下面利用其它思路，给出对合 C-H 矩阵的构造方法。

定义 5 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$h_1,h_2,\cdots,h_m\in\text{GF}(2^n)\setminus\{0\}$，使得对$0\le i,j\le m-1$，均有$b_{i,j}=a_{i,j}h_j$，则称矩阵$\boldsymbol{A}$与$\boldsymbol{B}$等效。

下面分析等效矩阵的密码学意义。

考察密码变换$(F_1(x_1),F_2(x_2),\cdots,F_m(x_m))=\boldsymbol{B}(S_1(x_1),S_2(x_2),\cdots,S_m(x_m))^{\text{T}}$。记$S_j'(z)=h_jS_j(z)$，则

$$F_i(x)=\overset{m}{\underset{j=0}{\oplus}}b_{i,j}S_j(x_j)=\overset{m}{\underset{j=0}{\oplus}}a_{i,j}h_jS_j(x_j)=\overset{m}{\underset{j=0}{\oplus}}a_{i,j}S_j'(x_j)$$

故有$(F_1(x_1),F_2(x_2),\cdots,F_m(x_m))=\boldsymbol{A}(S_1'(x_1),S_2'(x_2),\cdots,$

$S'_m(x_m))^{\mathrm{T}}$，这说明以线性变换 $\psi(\boldsymbol{x})=\boldsymbol{B}\boldsymbol{x}^{\mathrm{T}}$ 为扩散结构的 S-P 网络，就是使用以线性变换 $\varphi(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}^{\mathrm{T}}$ 为扩散结构，且将诸 S 盒 $S_j(z)$ 换为 $h_jS_j(z)$ 的S-P网络。这表明由等效扩散结构定义的 S-P 网络本质上相同。由引理 1 易证。

定理 7　GF(2^n) 上等效矩阵具有相同的差分分支数和线性分支数。

定理 8　任一个C-H矩阵都与一个对合C-H矩阵等效。

证明　设 $\boldsymbol{A}=(a_{i,j})_{2^m\times 2^m}$ 是 GF(2^n) 上基于 $(\delta,x_0,\cdots,x_{2^m-1})$ 构造的 C-H 矩阵，令 $\beta=\overset{2^m-1}{\underset{i=0}{\oplus}}a_{0,i}$，则由定理 5 和 Cauchy 矩阵的可逆性知 $\beta\neq 0$。由

$$\beta^{-1}a_{i,j}=\beta^{-1}(x_i\oplus x_j\oplus\delta)^{-1}=(\beta x_i\oplus\beta x_j\oplus\beta\delta)^{-1}$$

知 $\boldsymbol{B}=(\beta a_{i,j})_{2^m\times 2^m}$ 是 GF(2^n) 上基于 $(\beta\delta,\beta x_0,\cdots,\beta x_{2^m-1})$ 构造的 C-H 矩阵，再由定理 5 知

$$\boldsymbol{B}^2=\left[\overset{2^m-1}{\underset{i=0}{\oplus}}(\beta a_{0,i})^2\right]\boldsymbol{E}=\left[\beta^2\overset{2^m-1}{\underset{i=0}{\oplus}}a_{0,i}^2\right]\boldsymbol{E}$$
$$=\left[\beta^2\left(\overset{2^m-1}{\underset{i=0}{\oplus}}a_{0,i}\right)^2\right]\boldsymbol{E}=\boldsymbol{E}$$

这说明 $\beta^{-1}\boldsymbol{A}$ 是对合的 C-H 矩阵。　　证毕

定理 8 解决了如何构造对合 C-H 矩阵的问题。由于C-H矩阵都与一个对合C-H矩阵等效，且 $\beta^{-1}\boldsymbol{A}$ 与 $\boldsymbol{A}$ 具有相近的实现性能，因而在分组密码的设计中，可以只使用对合 C-H 矩阵形成的对合 MDS 矩阵，而不必使用非对合的 C-H 矩阵。

5　结束语

本文研究了结合 Cauchy 矩阵和 Hadamard 矩阵构造 MDS 矩阵的问题，解决了 Cauchy-Hadamard 矩阵的结构、构造方法和计数问题，证明了任一个 Cauchy-Hadamard 矩阵都等效于一个对合的 Cauchy-Hadamard 矩阵，并给出了相应的转化方法。本文的研究结果为 MDS 矩阵和对合 MDS 矩阵的构造提供了一种新的途径，在分组密码的设计中具有实际的应用价值。

参 考 文 献

[1] Schneier B, Kelsey J, and Whiting D, *et al*.. Twofish: A 128-bit block cipher. Available at http://www.schneier.com/, 2007-2-2.

[2] Wang Mei-qin. Differential cryptanalysis of present. Cryptology ePrint Archive, Report 2007/408.

[3] Wu Wen-ling, Zhang Wen-tao, and Feng Deng-guo. Impossible differential cryptanalysis of reduce round ARIA and camellia. *Journal of Computer Science and Technology*, 2007, 22(3): 449–456.

[4] Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. [Ph.D. dissertation], KU, Leuven, 1995.

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

[6] Xiao L and Heys H. Hardware design and analysis of block cipher components. Proceedings of the 5th International Conference on Information Security and Cryptology-ICISC'02, 2003 LNCS 2587: 164–181.

[7] 王念平, 金晨辉, 余昭平. 对合型列混合变换的研究. 电子学报, 2005, 33(10): 1917–1920.

Wang N P , Jin C H, and Yu Z P. Research on involution-typed mixcolumn transform. *Acta Electronica Sinica*, 2005, 33(10): 1917–1920.

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

[9] Blomer J, Kalfane M, and Karpinski M, *et al*.. An Xor-based erasure-resilient coding scheme. Technical Report TR-95-048. International Computer Science Institute, August 1995.

崔　霆：　男，1985 年生，硕士生，研究方向为密码学.

金晨辉：　男，1965 年生，教授，博士生导师，研究方向为密码学与信息安全.