MDS 矩阵和对合 MDS 矩阵的新构造方法*

郭 磊[1]，郑浩然[1]，傅增强[2]，王 月[1]
（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：首先对 Lacan 等人给出的由 Vandermonde 矩阵构造 MDS 码的方法进行了研究，指出了其中存在的问题，给出了由两个 Vandermonde 矩阵构造 MDS 矩阵的充要条件；然后利用矩阵乘的方法，给出了由标量乘 Vandermonde 矩阵构造 MDS 矩阵的充要条件；最后在 Sajadieh 等人给出的由两个 Vandermonde 矩阵构造对合 MDS 矩阵方法的基础之上，给出了标量乘 Vandermonde 矩阵构造对合 MDS 矩阵的方法。对标量乘矩阵来讲，可以通过调控标量中分量的大小来调整标量乘矩阵元素大小和元素重量大小来满足其软、硬件实现性能，因此该构造 MDS 矩阵及对合 MDS 矩阵的方法具有实用价值。

关键词：分组密码；扩散结构；分支数；MDS 矩阵；Vandermonde 矩阵
中图分类号：TP309.7 **文献标志码**：A **文章编号**：1001-3695(2014)01-0222-04
doi:10.3969/j.issn.1001-3695.2014.01.052

New construction methods for MDS matrices and involution MDS matrices

GUO Lei[1], ZHENG Hao-ran[1], FU Zeng-qiang[2], WANG Yue[1]
(1. *Institution No.* 3, *Information Engineering University*, *Zhengzhou* 450004, *China*; 2. *The Air Force Xi'an Flight Academy*, *Xi'an* 710300, *China*)

Abstract: Firstly this paper studied the method of constructing MDS codes by Vandermonde matrices proposed by Lacan et al and point out the problems existing in this method, and proposed the necessary and sufficient conditions of constructing MDS matrices by two Vandermonde matrices. Then, using the method of matrix multiplication, this paper proposed the necessary and sufficient conditions of constructing MDS matrices by scalar multiplication Vandermonde matrices. Finally, based on the method of constructing involution MDS matrices from two Vandermonde matrices proposed by Sajadieh et al, this paper proposed the method of constructing involution MDS matrices by scalar multiplication Vandermonde matrices. For scalar multiplication matrices, it could adjust elements size and weight in scalar multiplication matrices through regulating the size of scalar components to meet the implementation performance of software and hardware. So the methods of constructing MDS matrices and involution MDS matrices have practical value.

Key words: block cipher; diffusion structure; branch number; MDS(maximum distance separable) matrices; Vandermonde matrices

0 引言

混乱原则和扩散原则是保证分组密码安全性的两个基本设计原则。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]。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[2,3]。以分支数尽可能大的线性变换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 MDS 矩阵的分支数达到了最大，使得 MDS 矩阵在分组密码扩散结构的设计中得到广泛应用，如 AES[4]、Khazad[5] 和 Shark 等分组密码算法等。此外，为了保证加脱密结构的一致性，MDS 矩阵最好是对合矩阵，因此，如何构造对合型 MDS 矩阵显得尤为重要。

常见的 MDS 矩阵构造方法主要有三种：a）利用纠错码理论，从 MDS 码中提取 MDS 矩阵，如 AES、Khazad、Shark 等分组密码就是通过分组码理论来构造它们扩散层中使用的 MDS 矩阵。文献[6]给出了一种利用两个 Vandermonde 矩阵构造 MDS 码的方法，但在其 Vandermonde 矩阵的定义下，文献中的构造方法是有缺陷的；文献[7]给出了从线性分组码中搜索 MDS 矩阵的三种方法。b）随机生成 MDS 矩阵，如：文献[8]指出可以从循环矩阵、Hadamard 矩阵以及 Cauchy 矩阵中搜索便于实现的 MDS 矩阵；文献[9]通过限制条件在 Cauchy 矩阵中搜索出了 16×16 的对合 MDS 矩阵。c）利用数学方法构造 MDS 矩阵，如：文献[10]利用代数方法，给出了一种构造对合 Cauchy-Hadamard 型 MDS 矩阵的方法；文献[11]给出了利用两个 Vandermonde 矩阵构造对合 MDS 矩阵。

一般来说，由于已知的 MDS 码不多，并且利用方法 a）构造出的 MDS 矩阵，其软、硬件实现性能未必能满足要求；利用方法 b）构造出的 MDS 矩阵，当矩阵的阶数和 n（矩阵中的元素属于有限域 $GF(2^n)$）较大时，直接进行随机搜索显得不太现实，此时，密码上一般在具有特定结构的矩阵中进行搜索，但是当矩阵的阶数和 n 较大时，直接搜索也变得异常困难；利用方

收稿日期：2013-03-30；**修回日期**：2013-04-28 **基金项目**：国家自然科学基金资助项目(6127041)

作者简介：郭磊(1986-)，男，甘肃兰州人，硕士，主要研究方向为密码学(gl200644@163.com)；郑浩然(1968-)，男，教授，博士，主要研究方向为密码学、信息安全；傅增强(1979-)，男，助理工程师，主要研究方向为信息安全；王月(1986-)，男，硕士研究生，主要研究方向为密码学.

法 c)构造出的 MDS 矩阵往往具有特定的数学结构,其软、硬件实现性能也未必能满足要求。

本文对文献[6]中存在的问题进行了纠正,给出了正确的利用两个 Vandermonde 矩阵构造 MDS 矩阵的方法;考虑到利用该方法构造出的 MDS 矩阵的软、硬件实现性能,对标量乘 Vandermonde 矩阵构造 MDS 矩阵进行了研究,给出了由标量乘 Vandermonde 矩阵构造 MDS 矩阵的充要条件;在文献[11]给出的构造对合 MDS 矩阵方法的基础之上,给出了特征为 2 的域上标量乘 Vandermonde 矩阵构造对合 MDS 矩阵的方法。

1　基础知识

本文从矩阵角度来介绍差分分支数与线性分支数。

定义 1[12]　设 $\boldsymbol{x}=(x_1,\cdots,x_m)\in GF(2^n)^m$,则称 $x_1,\cdots,x_m$ 中非零元的个数为 $\boldsymbol{x}$ 的汉明重量,简称为重量,记为 $w(\boldsymbol{x})$。

定义 2[12]　令 $\theta:GF(2^n)^m\to GF(2^n)^m\boldsymbol{x}\to\theta(\boldsymbol{x})=\boldsymbol{A}\times\boldsymbol{x}$ 是一个变换,$\boldsymbol{x}=(x_1,\cdots,x_m)^{\mathrm{T}}\in GF(2^n)^m$,矩阵 $\boldsymbol{A}=(a_{ij})_{m\times m}$,$a_{ij}\in GF(2^n)$,则称

$$B(\boldsymbol{A})=\min_{x\neq 0}\{w(\boldsymbol{x})+w(\boldsymbol{A}\times\boldsymbol{x})\}$$

为 $\boldsymbol{A}$ 的分支数。

定义 3[12]　令 $\theta:GF(2^n)^m\to GF(2^n)^m\boldsymbol{x}\to\theta(\boldsymbol{x})=\boldsymbol{A}\times\boldsymbol{x}$ 是一个变换,$\boldsymbol{x}=(x_1,\cdots,x_m)^{\mathrm{T}}\in GF(2^n)^m$,$\boldsymbol{x}^*=(x_1^*,\cdots,x_m^*)^{\mathrm{T}}\in GF(2^n)^m$,矩阵 $\boldsymbol{A}=(a_{ij})_{m\times m}$,$a_{ij}\in GF(2^n)$,则称

$$B_d(\boldsymbol{A})=\min_{\boldsymbol{x},\boldsymbol{x}\neq\boldsymbol{x}^*}\{w(\boldsymbol{x}\oplus\boldsymbol{x}^*)+w(\boldsymbol{A}\times\boldsymbol{x}\oplus\theta(\boldsymbol{A}\times\boldsymbol{x}^*))\}$$

为 $\boldsymbol{A}$ 的差分分支数。

定义 4[12]　令 $\theta:GF(2^n)^m\to GF(2^n)^m\boldsymbol{x}\to\theta(\boldsymbol{x})=\boldsymbol{A}\times\boldsymbol{x}$ 是一个变换,$\boldsymbol{x}=(x_1,\cdots,x_m)^{\mathrm{T}}\in GF(2^n)^m$,$\beta=(\beta_1,\cdots,\beta_m)^{\mathrm{T}}\in GF(2^n)^m$,矩阵 $\boldsymbol{A}=(a_{ij})_{m\times m}$,$a_{ij}\in GF(2^n)$,则称

$$B_l(\boldsymbol{A})=\min_{\beta\neq 0}\{w(\beta)+w(\boldsymbol{A}^{\mathrm{T}}\times\beta)\},$$

为 $\boldsymbol{A}$ 的线性分支数($\boldsymbol{A}^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{A}$ 的转置矩阵)。

对任意矩阵 $\boldsymbol{A}$,由于 $\boldsymbol{A}\times a\oplus\boldsymbol{A}\times b=\boldsymbol{A}\times(a\oplus b)$,因此差分分支数与分支数是一致的,而线性分支数与分支数不一定相等。但对于 MDS 矩阵来讲,其差分分支数与线性分支数是相等的。

由于密码学中应用的 MDS 矩阵与分组码理论中的 MDS 码是相对应的,因此本文简要介绍有关分组码的基础知识:有限域 $GF(q)$ 上的一个 $[n,k,d]$-线性码是向量空间 $GF(q)^n$ 一个 k 维子空间,两个 n 维向量的最小汉明距离即两个码字的最小汉明距离为 d。一个 $[n,k,d]$-线性码 C 的生成矩阵 $\boldsymbol{G}$ 是一个由 C 的一组基作为矩阵的行而形成的一个 $k\times n$ 矩阵。若一个 $[n,k,d]$-线性码的生成矩阵 $\boldsymbol{G}=[E_{k\times k}\mid\boldsymbol{A}]$,其中,$E_{k\times k}$ 为 $k\times k$ 的单位矩阵,$\boldsymbol{A}$ 是一 $k\times(n-k)$ 矩阵,那么生成矩阵 $\boldsymbol{G}$ 称为 $[n,k,d]$-线性码的标准生成矩阵。$[n,k,d]$-线性码遵循 Singleton 界,$d\leqslant n-k+1$,本文把 $d=n-k+1$ 的 $[n,k,d]$-线性码称为极大最小距离可分码(maximum distance separable codes,MDS)[13]。分组密码设计中应用的 MDS 矩阵即为 MDS 码的标准生成矩阵 $\boldsymbol{G}=[I_{k\times k}\mid\boldsymbol{A}]$ 中的矩阵 $\boldsymbol{A}$,一般取 $n=2k$,因此有关 MDS 码的相关结论直接应用到 MDS 矩阵的证明中。

引理 1[13]　设 $\boldsymbol{A}$ 为有限域 $GF(q)$ 上的 n 阶方阵,以下三个条件是等价的:a)$\boldsymbol{A}$ 是 MDS 矩阵;b)矩阵 $[E_n\mid\boldsymbol{A}]$ 中任意的 n 列是线性无关的;c)矩阵 $[-\boldsymbol{A}^{\mathrm{T}}\mid E_n]$ 中任意的 n 列是线性无关的。

引理 2[13]　有限域 $GF(q)$ 上的 n 阶方阵 $\boldsymbol{A}$ 是 MDS 矩阵的充要条件是矩阵 $\boldsymbol{A}$ 的任意阶子方阵都是非奇异的。

定义 5[13]　设 $a_i\in GF(q)$,$i=1,\cdots,m$,q 为素数或素数的方幂,则由 $GF(q)^n$ 中的向量 $(a_1,\cdots,a_m)$ 决定的 Vandermonde 方阵

$$V(a_1,\cdots,a_m)=(a_j^{i-1})_{i,j=1}^m=\begin{pmatrix}1&1&\cdots&1\\a_1&a_2&\cdots&a_m\\\vdots&\vdots&&\vdots\\a_1^{m-1}&a_2^{m-1}&\cdots&a_m^{m-1}\end{pmatrix}。$$

Vandermonde 方阵的行列式 $\det(V(a_1,\cdots,a_m))=\prod_{1\leqslant i<j\leqslant m}(a_j-a_i)$,其中 $m\geqslant 2$。

若可逆矩阵

$$\boldsymbol{A}=(a_i^{j-1})_{i,j=1}^m=\begin{pmatrix}1&a_1&\cdots&a_1^{m-1}\\1&a_2&\cdots&a_2^{m-1}\\\vdots&\vdots&&\vdots\\1&a_m&\cdots&a_m^{m-1}\end{pmatrix}$$

$$\boldsymbol{B}=(b_i^{j-1})_{i,j=1}^m=\begin{pmatrix}1&b_1&\cdots&b_1^{m-1}\\1&b_2&\cdots&b_2^{m-1}\\\vdots&\vdots&&\vdots\\1&b_m&\cdots&b_m^{m-1}\end{pmatrix}$$

显然矩阵

$$\begin{pmatrix}1&a_1&\cdots&a_1^{m-1}&1&b_1&\cdots&b_1^{m-1}\\1&a_2&\cdots&a_2^{m-1}&1&b_2&\cdots&b_2^{m-1}\\\vdots&\vdots&&\vdots&\vdots&\vdots&&\vdots\\1&a_m&\cdots&a_m^{m-1}&1&b_m&\cdots&b_m^{m-1}\end{pmatrix}$$

中存在奇异的 m 阶子方阵,如其前 $m-1$ 列和第 $m+1$ 构成的 m 阶子方阵

$$\begin{pmatrix}1&a_1&\cdots&a_1^{m-2}&1\\1&a_2&\cdots&a_2^{m-2}&1\\\vdots&\vdots&&\vdots&\vdots\\1&a_m&\cdots&a_m^{m-2}&1\end{pmatrix}$$

就是奇异的。那么矩阵 $\boldsymbol{A}^{-1}(\boldsymbol{A}\mid\boldsymbol{B})=(E\mid\boldsymbol{A}^{-1}\boldsymbol{B})$ 中存在奇异的 m 阶子方阵,根据引理 1 知矩阵 $\boldsymbol{A}^{-1}\boldsymbol{B}$ 非 MDS 矩阵,进而根据引理 2 知矩阵 $\boldsymbol{A}^{-1}\boldsymbol{B}$ 中存在奇异的子方阵。而文献[6]中的 Vandermonde 矩阵的定义即为

$$V(a_1,\cdots,a_m)=(a_i^{j-1})_{i,j=1}^m=\begin{pmatrix}1&a_1&\cdots&a_1^{m-1}\\1&a_2&\cdots&a_2^{m-1}\\\vdots&\vdots&&\vdots\\1&a_m&\cdots&a_m^{m-1}\end{pmatrix}$$

这种形式,因此文献[6]中的定理 1、2 是有问题的。

定理 1[6]　记 $V(a_1,\cdots,a_r)$ 为 Vandermonde 矩阵 $(a_i^{j-1})_{i,j=1}^m$,则对 $(F_q)^r$ 上的任意两个向量 $(a_1,\cdots,a_r)$ 和 $(b_1,\cdots,b_r)$,若 a_i,b_j 是 $2r$ 个互不相同的元,那么矩阵

$$V(a_1,\cdots,a_r)^{-1}V(b_1,\cdots,b_r)$$

中的任意一个子方阵都是非奇异的。

定理 2[6]　记 $V(a_1,\cdots,a_k)$ 为 $k\times k$ 的非奇异 Vandermonde 矩阵,$V(b_1,\cdots,b_{n-k})$ 为 $k\times(n-k)$ 矩阵 $(b_i^{j-1})_{i=1,\cdots,n-k}^{j=1,\cdots,k}$,则由生成矩阵 $\boldsymbol{G}=[E_k\mid V(a_1,\cdots,a_k)^{-1}V(b_1,\cdots,b_{n-k})]$ 定义的码为 MDS 码的充要条件为 a_i、b_j 是 n 个互不相同的元。

2　由 Vandermonde 矩阵构造 MDS 矩阵

下面给出正确的由两个 Vandermonde 矩阵构造 MDS 矩阵的充要条件:

定理 3　设有限域 $GF(q)$ 上的 Vandermonde 方阵 $V(a_1,\cdots,a_m)=(a_j^{i-1})_{i,j=1}^m$,$V(b_1,\cdots,b_m)=(b_j^{i-1})_{i,j=1}^m$,则矩阵 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$ 是 MDS 矩阵的充要条件是 a_i,b_j 为 $GF(q)$ 中 $2m$ 互不相同的元。

证明　必要性。证明若 $GF(q)$ 上的矩阵 $V(a_1,\cdots,a_m)^{-1}$

$V(b_1,\cdots,b_m)$是 MDS 矩阵,那么 a_i、b_j 为 $GF(q)$中 $2m$ 互不相同的元。

根据引理 1 可知,若 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$是 MDS 矩阵,那么矩阵$[E\mid V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)]$中任意的 m 阶子方阵是非奇异的,而矩阵

$$V(a_1,\cdots,a_m)[E\mid V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m))=[V(a_1,\cdots,a_m)\mid V(b_1,\cdots,b_m)]$$

因此矩阵$[V(a_1,\cdots,a_m)\mid V(b_1,\cdots,b_m)]$中任意的 m 阶子方阵也是非奇异的,而矩阵$[V(a_1,\cdots,a_m)\mid V(b_1,\cdots,b_m)]$中任意的 m 阶子方阵正好也是一个 Vandermonde 方阵,由 Vandermonde 方阵的行列式知 Vandermonde 方阵的行列式不等于零当且仅当 Vandermonde 方阵的生成向量中的元互不相等,因此 a_i、b_j 为 $GF(q)$中 $2m$ 互不相同的元。

充分性。即证明若 a_i、b_j 为 $GF(q)$中 $2m$ 互不相同的元,那么矩阵 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$是 MDS 矩阵。

显然矩阵$[V(a_1,\cdots,a_m)\mid V(b_1,\cdots,b_m)]$中任意的 m 阶子方阵仍为一个 Vandermonde 方阵,由 a_i、b_j 为 $GF(q)$中 $2m$ 互不相同的元知$[V(a_1,\cdots,a_m)\mid V(b_1,\cdots,b_m)]$中任意的 m 阶子方阵都是非奇异,则矩阵

$$V(a_1,\cdots,a_m)^{-1}[V(a_1,\cdots,a_m)\mid V(b_1,\cdots,b_m)]=[E\mid V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)]$$

中任意的 m 阶子方阵也是非奇异的,根据引理 1 知矩阵 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$为 MDS 矩阵。证毕。

由定理 1 和文献[6]中的定理 2 知:

若 $GF(q)$上的矩阵 $V(a_1,\cdots,a_m)=(a_j^{i-1})_{i,j=1}^m$,$V(b_1,\cdots,b_m)=(b_j^{i-1})_{i,j=1}^m$,则矩阵 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$为 MDS 矩阵充要条件是 a_i、b_j 为 $GF(q)$中 $2m$ 互不相同的元;

若 $GF(q)$上的矩阵 $V(a_1,\cdots,a_m)=(a_i^{j-1})_{i,j=1}^m$,$V(b_1,\cdots,b_m)=(b_i^{j-1})_{i,j=1}^m$,则矩阵 $V(a_1,\cdots,a_m)V(b_1,\cdots,b_m)^{-1}$为 MDS 矩阵充要条件是 a_i、b_j 为 $GF(q)$中 $2m$ 互不相同的元。

3 标量乘 Vandermonde 矩阵构造 MDS 矩阵

在有限域 $GF(q)$上,记

$$A^{(\alpha_1,\cdots,\alpha_m)}=\begin{pmatrix}\alpha_1a_{1,1}&\cdots&\alpha_ma_{1,m}\\ \vdots&&\vdots\\ \alpha_1a_{m,1}&\cdots&\alpha_ma_{m,m}\end{pmatrix}$$

为标量$(\alpha_1,\cdots,\alpha_m)$乘矩阵

$$A=(a_{i,j})_{i,j=1}^m=\begin{pmatrix}a_{1,1}&\cdots&a_{1,m}\\ \vdots&&\vdots\\ a_{m,1}&\cdots&a_{m,m}\end{pmatrix}$$

的标量乘矩阵,记

$$A^{(\alpha_1,\cdots,\alpha_m)^{\mathrm{T}}}=\begin{pmatrix}\alpha_1a_{1,1}&\cdots&\alpha_1a_{1,m}\\ \vdots&&\vdots\\ \alpha_ma_{m,1}&\cdots&\alpha_ma_{m,m}\end{pmatrix}$$

为了研究标量乘 Vandermonde 方阵构造 MDS 矩阵的方法,下面首先分别由定理 1 给出标量乘矩阵逆的结构特点,由定理 2 给出两个矩阵相乘与它们的标量乘矩阵相乘的关系,再由定理 4 给出由两个标量乘 Vandermonde 方阵构造 MDS 的充要条件。

定理 4 $(A^{(\alpha_1,\cdots,\alpha_m)})^{-1}=(A^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}}$。

证明 设 $A^{-1}=T=(t_{i,j})_{i,j=1}^m$,由

$$A^{-1}A=\begin{pmatrix}t_{1,1}&\cdots&t_{1,m}\\ \vdots&&\vdots\\ t_{m,1}&\cdots&t_{m,m}\end{pmatrix}\begin{pmatrix}a_{1,1}&\cdots&a_{1,m}\\ \vdots&&\vdots\\ a_{m,1}&\cdots&a_{m,m}\end{pmatrix}=E$$

知

$$(A^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}}A^{(\alpha_1,\cdots,\alpha_m)}=\begin{pmatrix}\alpha_1^{-1}t_{1,1}&\cdots&\alpha_1^{-1}t_{1,m}\\ \vdots&&\vdots\\ \alpha_m^{-1}t_{m,1}&\cdots&\alpha_m^{-1}t_{m,m}\end{pmatrix}\begin{pmatrix}\alpha_1a_{1,1}&\cdots&\alpha_ma_{1,m}\\ \vdots&&\vdots\\ \alpha_1a_{m,1}&\cdots&\alpha_ma_{m,m}\end{pmatrix}=E$$

由

$$AA^{-1}=\begin{pmatrix}a_{1,1}&\cdots&a_{1,m}\\ \vdots&&\vdots\\ a_{m,1}&\cdots&a_{m,m}\end{pmatrix}\begin{pmatrix}t_{1,1}&\cdots&t_{1,m}\\ \vdots&&\vdots\\ t_{m,1}&\cdots&t_{m,m}\end{pmatrix}=E$$

知

$$A^{(\alpha_1,\cdots,\alpha_m)}(A^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}}=\begin{pmatrix}\alpha_1a_{1,1}&\cdots&\alpha_ma_{1,m}\\ \vdots&&\vdots\\ \alpha_1a_{m,1}&\cdots&\alpha_ma_{m,m}\end{pmatrix}\begin{pmatrix}\alpha_1^{-1}t_{1,1}&\cdots&\alpha_1^{-1}t_{1,m}\\ \vdots&&\vdots\\ \alpha_m^{-1}t_{m,1}&\cdots&\alpha_m^{-1}t_{m,m}\end{pmatrix}=E$$

因此

$$(A^{(\alpha_1,\cdots,\alpha_m)})^{-1}=\begin{pmatrix}\alpha_1^{-1}t_{1,1}&\cdots&\alpha_1^{-1}t_{1,m}\\ \vdots&&\vdots\\ \alpha_m^{-1}t_{m,1}&\cdots&\alpha_m^{-1}t_{m,m}\end{pmatrix}=(A^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}}$$

证毕。

定理 5 若 $A=(a_{i,j})_{i,j=1}^m$,$B=(b_{i,j})_{i,j=1}^m$,则

$$(A^{(\alpha_1,\cdots,\alpha_m)})^{-1}B^{(\beta_1,\cdots,\beta_m)}=((A^{-1}B)^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}})^{(\beta_1,\cdots,\beta_m)}$$

证明 设 $A^{-1}=T=(t_{i,j})_{i,j=1}^m$,则由定理 1 知

$$(A^{(\alpha_1,\cdots,\alpha_m)})^{-1}B^{(\beta_1,\cdots,\beta_m)}=(A^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}}B^{(\beta_1,\cdots,\beta_m)}$$

矩阵$(A^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}}B^{(\beta_1,\cdots,\beta_m)}$中第 i 行第 j 列的元为$\sum_{k=1}^m\alpha_i^{-1}t_{i,k}\beta_jb_{k,j}$。

显然 $A^{-1}B$ 中第 i 行第 j 列的元为$\sum_{k=1}^m t_{i,k}b_{k,j}$,那么$((A^{-1}B)^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}})^{(\beta_1,\cdots,\beta_m)}$中第 i 行第 j 列的元为 $\alpha_i^{-1}\beta_j\sum_{k=1}^m t_{i,k}b_{k,j}$,这与矩阵$(A^{-1})^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}}B^{(\beta_1,\cdots,\beta_m)}$中第 i 行第 j 列的元$\sum_{k=1}^m\alpha_i^{-1}t_{i,k}\beta_jb_{k,j}$相等,即与$(A^{(\alpha_1,\cdots,\alpha_m)})^{-1}B^{(\beta_1,\cdots,\beta_m)}$第 i 行第 j 列的元$\sum_{k=1}^m\alpha_i^{-1}t_{i,k}\beta_jb_{k,j}$相等,由 i、j 的任意性知$(A^{(\alpha_1,\cdots,\alpha_m)})^{-1}B^{(\beta_1,\cdots,\beta_m)}=((A^{-1}B)^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}})^{(\beta_1,\cdots,\beta_m)}$。证毕。

定理 6 设有限域 $GF(q)$的 Vandermonde 方阵 $V(a_1,\cdots,a_m)=(a_j^{i-1})_{i,j=1}^m$,$V(b_1,\cdots,b_m)=(b_j^{i-1})_{i,j=1}^m$,则矩阵$(V(a_1,\cdots,a_m)^{(\alpha_1,\cdots,\alpha_m)})^{-1}V(b_1,\cdots,b_m)^{(\beta_1,\cdots,\beta_m)}$是 MDS 矩阵的充要条件是 a_i、b_j 为 $GF(q)$中 $2m$ 互不相同的元且 α_i、β_j 都为非零元。

证明 根据引理 2 知矩阵$(V(a_1,\cdots,a_m)^{(\alpha_1,\cdots,\alpha_m)})^{-1}V(b_1,\cdots,b_m)^{(\beta_1,\cdots,\beta_m)}$是 MDS 矩阵的充要条件是其任意阶子方阵都是非奇异的。

根据定理 3 知

$$(V(a_1,\cdots,a_m)^{(\alpha_1,\cdots,\alpha_m)})^{-1}V(b_1,\cdots,b_m)^{(\beta_1,\cdots,\beta_m)}=((V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m))^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}}})^{(\beta_1,\cdots,\beta_m)}$$

为了证明方便不妨记矩阵 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$中任意的 k 阶子方阵为 $T=(t_{i_h,j_l})_{h,l=1}^k$,那么矩阵$(V(a_1,\cdots,a_m)^{(\alpha_1,\cdots,\alpha_m)})^{-1}V(b_1,\cdots,b_m)^{(\beta_1,\cdots,\beta_m)}$中任意的 k 阶子式即为

$$\begin{vmatrix}\alpha_{i_1}^{-1}\beta_{j_1}t_{i_1,j_1}&\alpha_{i_1}^{-1}\beta_{j_2}t_{i_1,j_2}&\cdots&\alpha_{i_1}^{-1}\beta_{j_k}t_{i_1,j_k}\\ \alpha_{i_2}^{-1}\beta_{j_1}t_{i_2,j_1}&\alpha_{i_2}^{-1}\beta_{j_2}t_{i_2,j_2}&\cdots&\alpha_{i_2}^{-1}\beta_{j_k}t_{i_2,j_k}\\ \vdots&\vdots&&\vdots\\ \alpha_{i_k}^{-1}\beta_{j_1}t_{i_k,j_1}&\alpha_{i_k}^{-1}\beta_{j_2}t_{i_k,j_2}&\cdots&\alpha_{i_k}^{-1}\beta_{j_k}t_{i_k,j_k}\end{vmatrix}$$

根据行列式的性质知

$$\begin{vmatrix} \alpha_{i_1}^{-1}\beta_{j_1}t_{i_1,j_1} & \alpha_{i_1}^{-1}\beta_{j_2}t_{i_1,j_2} & \cdots & \alpha_{i_1}^{-1}\beta_{j_k}t_{i_1,j_k} \\ \alpha_{i_2}^{-1}\beta_{j_1}t_{i_2,j_1} & \alpha_{i_2}^{-1}\beta_{j_2}t_{i_2,j_2} & \cdots & \alpha_{i_2}^{-1}\beta_{j_k}t_{i_2,j_k} \\ \vdots & \vdots & & \vdots \\ \alpha_{i_k}^{-1}\beta_{j_1}t_{i_k,j_1} & \alpha_{i_k}^{-1}\beta_{j_2}t_{i_k,j_2} & \cdots & \alpha_{i_k}^{-1}\beta_{j_k}t_{i_k,j_k} \end{vmatrix} = \alpha_{i_1}^{-1}\cdots\alpha_{i_k}^{-1}\beta_{j_1}\cdots\beta_{j_k}\begin{vmatrix} t_{i_1,j_1} & t_{i_1,j_2} & \cdots & t_{i_1,j_k} \\ t_{i_2,j_1} & t_{i_2,j_2} & \cdots & t_{i_2,j_k} \\ \vdots & \vdots & & \vdots \\ t_{i_k,j_1} & t_{i_k,j_2} & \cdots & t_{i_k,j_k} \end{vmatrix},$$

而

$$\alpha_{i_1}^{-1}\cdots\alpha_{i_k}^{-1}\beta_{j_1}\cdots\beta_{j_k}\begin{vmatrix} t_{i_1,j_1} & t_{i_1,j_2} & \cdots & t_{i_1,j_k} \\ t_{i_2,j_1} & t_{i_2,j_2} & \cdots & t_{i_2,j_k} \\ \vdots & \vdots & & \vdots \\ t_{i_k,j_1} & t_{i_k,j_2} & \cdots & t_{i_k,j_k} \end{vmatrix} \neq 0$$

当且仅当 α_{i_h},β_{j_l}是非零元 $h,l=1,\cdots,k$,且

$$\begin{vmatrix} t_{i_1,j_1} & t_{i_1,j_2} & \cdots & t_{i_1,j_k} \\ t_{i_2,j_1} & t_{i_2,j_2} & \cdots & t_{i_2,j_k} \\ \vdots & \vdots & & \vdots \\ t_{i_k,j_1} & t_{i_k,j_2} & \cdots & t_{i_k,j_k} \end{vmatrix} \neq 0$$

根据引理 2 知

$$\begin{vmatrix} t_{i_1,j_1} & t_{i_1,j_2} & \cdots & t_{i_1,j_k} \\ t_{i_2,j_1} & t_{i_2,j_2} & \cdots & t_{i_2,j_k} \\ \vdots & \vdots & & \vdots \\ t_{i_k,j_1} & t_{i_k,j_2} & \cdots & t_{i_k,j_k} \end{vmatrix} \neq 0$$

当且仅当 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$是 MDS 矩阵,再根据定理 1 知矩阵 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$是 MDS 矩阵的充要条件为 a_i、b_j 为 $GF(q)$ 中 $2m$ 互不相同的元。因此$(V(a_1,\cdots,a_m)^{(\alpha_1,\cdots,\alpha_m)})^{-1}V(b_1,\cdots,b_m)^{(\beta_1,\cdots,\beta_m)}$是 MDS 矩阵的充要条件是 a_i,b_j 为 $GF(q)$中 $2m$ 互不相同的元且 α_i、β_j 都为非零元。证毕。

4　标量乘 Vandermonde 矩阵构造对合 MDS 矩阵

本章在文献[11]给出的由两个 Vandermonde 矩阵构造对合 MDS 矩阵方法的基础之上,给出有限域 $GF(2^n)$上由两个标量乘 Vandermonde 矩阵构造对合 MDS 矩阵的方法。

引理 3[11]　设有限域 $GF(2^n)$上的 Vandermonde 方阵

$$V(a_1,\cdots,a_m)=(a_j^{i-1})_{i,j=1}^m, V(b_1,\cdots,b_m)=(b_j^{i-1})_{i,j=1}^m$$

若 $b_i=a_i+\Delta$,则矩阵 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$为对合矩阵。

引理 4[11]　设有限域 $GF(2^n)$上的 Vandermonde 方阵

$$V(a_1,\cdots,a_m)=(a_j^{i-1})_{i,j=1}^m, V(b_1,\cdots,b_m)=(b_j^{i-1})_{i,j=1}^m$$

若 $b_i=a_i+\Delta$,且 a_i,b_j 为 $GF(2^n)$中 $2m$ 互不相同的元,则矩阵 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$为对合 MDS 矩阵。

定理 7　设有限域 $GF(2^n)$上的 Vandermonde 方阵

$V(a_1,\cdots,a_m)=(a_j^{i-1})_{i,j=1}^m, V(b_1,\cdots,b_m)=(b_j^{i-1})_{i,j=1}^m$,$(\alpha_1,\cdots,\alpha_m)\in GF(2^n)^m$,若 $b_i=a_i+\Delta$ 且 a_i,b_j 为 $GF(2^n)$中 $2m$ 互不相同的元,$\alpha_i\neq 0$,则矩阵$(V(a_1,\cdots,a_m)^{(\alpha_1,\cdots,\alpha_m)})^{-1}V(b_1,\cdots,b_m)^{(\alpha_1,\cdots,\alpha_m)}$为对合 MDS 矩阵。

证明　根据定理 6 知矩阵$(A^{(\alpha_1,\cdots,\alpha_m)})^{-1}B^{(\alpha_1,\cdots,\alpha_m)}$为 MDS 矩阵,下面证明其对合性质。

根据引理 3 知 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)$为对合矩阵,不妨设 $V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m)=T=(t_{i,j})_{i,j=1}^m$,则

$$(V(a_1,\cdots,a_m)^{(\alpha_1,\cdots,\alpha_m)})^{-1}V(b_1,\cdots,b_m)^{(\alpha_1,\cdots,\alpha_m)}=$$
$$((V(a_1,\cdots,a_m)^{-1}V(b_1,\cdots,b_m))^{(\alpha_1^{-1},\cdots,\alpha_m^{-1})^{\mathrm{T}})^{(\alpha_1,\cdots,\alpha_m)}}=$$
$$(\alpha_i^{-1}\alpha_j t_{i,j})_{i,j=1}^m,$$

那么矩阵$(\alpha_i^{-1}\alpha_j t_{i,j})_{i,j=1}^m$的第 i 行乘第 j 列后得到的元为

$$\sum_{k=1}^m \alpha_i^{-1}\alpha_k t_{i,k}\alpha_k^{-1}\alpha_j t_{k,j}=\sum_{k=1}^m t_{i,k}t_{k,j}=\begin{cases}1 & i=j\\ 0 & i\neq j\end{cases}$$

因此矩阵$(V(a_1,\cdots,a_m)^{(\alpha_1,\cdots,\alpha_m)})^{-1}V(b_1,\cdots,b_m)^{(\alpha_1,\cdots,\alpha_m)}$为对合矩阵。

综上所述,若 $b_i=a_i+\Delta$ 且 a_i、b_j 为 $GF(2^n)$中 $2m$ 互不相同的元,$\alpha_i\neq 0$,则矩阵$(V(a_1,\cdots,a_m)^{(\alpha_1,\cdots,\alpha_m)})^{-1}V(b_1,\cdots,b_m)^{(\alpha_1,\cdots,\alpha_m)}$为对合 MDS 矩阵。证毕。

5　结束语

本文对 Lacan 等人给出的由 Vandermonde 矩阵构造 MDS 码的方法进行了研究,指出了其中存在的问题,给出了由两个 Vandermonde 矩阵构造 MDS 矩阵的充要条件。进而对标量乘 Vandermonde 矩阵的结构特点进行了研究,给出了由标量乘 Vandermonde 矩阵构造 MDS 矩阵的充要条件。最后在 Sajadieh 等人给出的由两个 Vandermonde 矩阵构造对合 MDS 矩阵方法的基础之上,给出了标量乘 Vandermonde 矩阵构造对合 MDS 矩阵的方法。对由标量乘 Vandermonde 矩阵构造的 MDS 矩阵及对合 MDS 矩阵来讲,可以通过调控标量中分量的大小来调整构造出来的 MDS 矩阵及对合 MDS 矩阵元素大小和元素重量大小来满足其软、硬件实现性能,因此本文给出的构造 MDS 矩阵及对合 MDS 矩阵的方法具有实用价值。

参考文献:

[1] DAEMEN J, RIJMEN V. The wide trail design strategy[C]//Proc of the 8th IAM International Conference Cirencester. Berlin: Springer-Verlag, 2001: 222-238.

[2] RIJMEN V, DAEMEN J, PRENEEL B, *et al*. The cipher SHARK [C]//Proc of Fast Software Encryption-FSE. [S. l.]: Springer-Verlag, 1996: 99-111.

[3] JU S K, SEOKHIE H, SANGJIN L, *et al*. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks[J]. ETRI Journal, 2001, 23(4): 158-167.

[4] DAEMEN J, RIJMEN V. The design of Rijndael: AES-the advanced encryption standard[M]. Berlin: Springer-Verlag, 2002.

[5] BARRETO P, RIJMEN V. The Khazad legacy-level block cipher [EB/OL]. (2000) [2006-12-03]. http://www. cryptonessie. org.

[6] JEROME L, JEROME F. Systematic MDS erasure codes based on vandermonde matrices[J]. IEEE Communications Letters, 2004, 8(9): 570-572.

[7] MATHUR C N, NARAYNA K, SUBBALAKSHMI K P. High diffusion cipher: encryption and error correction in a single cryptographic primitive[C]//LNCS, vol 3989. Berlin: Springer-Verlag, 2006: 309-324.

[8] XIAO L, HEYS H M. Hardware design and analysis of block cipher components[C]//Proc of the 5th International Conference on Information Security and Cryptology-ICISC. Berlin: Springer-Verlag, 2003: 164-181.

[9] JORGE N J, éLCIO A. A new involutory MDS matrix for the AES[J]. International Journal of Net Work Security, 2009, 9(2): 109-116.

[10] 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.

[11] SAJADIEH M, DAKHILALIAN M, MALA H, *et al*. On construction of involutory MDS matrices from Vandermonde Matrices in GF(2^q)[J]. Designs, Codes and Cryptography, 2012, 64(3): 287-308.

[12] 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.

[13] MCWILLIAMS F J, SLOANE N J A. The theory of error-correcting codes[M]. The Netherlands: North Holland, 1977.