具有最小异或数的最大距离可分矩阵的构造

陈少真 张怡帆* 任炯炯

(解放军信息工程大学 郑州 450001)

(数学工程与先进计算国家重点实验室 郑州 450001)

摘 要：随着物联网等普适计算的发展，传感器、射频识别(RFID)标签等被广泛使用，这些微型设备的计算能力有限，传统的密码算法难以实现，需要硬件效率高的轻量级分组密码来支撑。最大距离可分(MDS)矩阵扩散性能最好，通常被用于构造分组密码扩散层，异或操作次数(XORs)是用来衡量扩散层硬件应用效率的一个指标。该文利用一种能更准确评估硬件效率的XORs计算方法，结合一种特殊结构的矩阵——Toeplitz矩阵，构造XORs较少效率较高的MDS矩阵。利用Toeplitz矩阵的结构特点，改进矩阵元素的约束条件，降低矩阵搜索的计算复杂度，在有限域$\mathbb{F}_{2^8}$上得到了已知XORs最少的4×4MDS矩阵和6×6MDS矩阵，同时还得到XORs等于已知最优结果的5×5MDS矩阵。该文构造的具有最小XORs的MDS Toeplitz矩阵，对轻量级密码算法的设计具有现实意义。

关键词：分组密码；轻量级扩散层；最大距离可分矩阵；异或数；Toeplitz矩阵

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)10-2416-07

DOI: 10.11999/JEIT181113

Constructions of Maximal Distance Separable Matrices with Minimum XOR-counts

CHEN Shaozhen ZHANG Yifan REN Jiongjiong

(*PLA Information Engineering University*, *Zhengzhou* 450001, *china*)

(*State Key Laboratory of Mathematical Engineering and Advanced Computing*, *Zhengzhou* 450001, *china*)

Abstract: With the development of the internet of things, small-scale communication devices such as wireless sensors and the Radio Frequency IDentification(RFID) tags are widely used, these micro-devices have limited computing power, so that the traditional cryptographic algorithms are difficult to implement on these devices. How to construct a high-efficiency diffusion layer becomes an urgent problem. With the best diffusion property, the Maximal Distance Separable (MDS) matrix is often used to construct the diffusion layer of block ciphers. The number of XOR operations (XORs) is an indicator of the efficiency of hardware applications. Combined with the XORs calculation method which can evaluate hardware efficiency more accurately and a matrix with special structure——Toeplitz matrix, efficient MDS matrices with less XORs can be constructed. Using the structural characteristics of the Toeplitz matrix, the constraints of matrix elements are improved, and the complexity of matrices searching is reduced. The 4×4 MDS matrices and the 6×6 MDS matrices with the least XORs in the finite field $\mathbb{F}_{2^8}$ are obtained, and the 5×5 MDS matrices with the XORs which are equal to the known optimal results are obtained too. The proposed method of constructing MDS Toeplitz matrices with the least XORs has significance on the design of lightweight cryptographic algorithms.

Key words: Block cipher; Lightweight diffusion layers; Maximal Distance Separable(MDS) matrices; XOR-counts; Toeplitz matrices

收稿日期：2018-12-03；改回日期：2019-05-31；网络出版：2019-06-12

*通信作者： 张怡帆 zhangyifan_fan@163.com

基金项目：信息保障技术重点实验室开放基金(KJ-17-002)，国家密码发展基金(MMJJ20180203)，数学工程与先进计算国家重点实验室开放基金(2018A03)

Foundation Items: The Foundation of Science and Technology on Information Assurance Laboratory (KJ-17-002), The National Cipher Development Foundation (MMJJ20180203), The State Key Laboratory of Mathematical Engineering and Advanced Computation Open Foundation (2018A03)

1　引言

对称密码算法是现在几乎所有安全通信的基础，其中分组密码和Hash函数是对称密码学中的主力，主要用于进行加密和身份验证等。如今，可以选择较好的分组密码和Hash函数来抵抗较强的攻击。分组密码的设计原则易于理解，基于这些设计原则可以构造高效、简单和易于分析的密码。混淆和扩散是分组密码的两个重要标准，混淆层的作用是使密钥和明密文之间的关系尽可能复杂，扩散层为密码算法提供了内部独立性。

差分分析[1]和线性分析[2]是分组密码算法最有效的攻击方法，扩散层的输入差分和输出差分非0活动bit之和的最小值称为扩散层的差分分支数，输入掩码和输出掩码的非0活动bit之和的最小值为扩散层的线性分支数，利用它们可以给出分组密码活动S盒数目的界，进而衡量密码算法抵抗差分分析和线性分析的能力。因此分支数是衡量一个扩散层扩散性能好坏的指标，分支数越大，扩散效果越好，安全性越高。

最大距离可分矩阵(Maximal Distance Separable matrices)简称MDS矩阵，它的分支数达到最大，扩散效果最好，能更好的抵抗差分分析和线性分析，安全性最高，因此很多算法诸如AES(Advanced Encryption Standard)算法等采用MDS矩阵作为扩散层。

随着物联网等普适计算的发展，计算能力有限的微型设备被广泛应用，这对硬件提出了新的要求。许多传统密码算法效率较低，因此应用消耗较少的轻量级密码越来越受重视。轻量级分组密码如CLEFIA[3], PRESENT[4], LED[5], SIMECK[6]等被先后提出，其中前两个算法已经通过ISO/IEC29192标准。因为MDS矩阵的每一个元素均不为0，在应用时耗能较大，因此如何构造一个适用于轻量级密码算法的MDS矩阵受到了广泛关注。

扩散矩阵在应用时与输入向量进行矩阵乘法运算得到输出向量，2015年，文献[7]介绍了一个衡量硬件应用效率的指标异或数(XORs), XORs就是扩散矩阵在应用时所需要进行的异或操作次数，XORs越少，应用效率越高。

XORs较少的MDS矩阵能更好地保证扩散层的安全性与效率，在实现最佳扩散性能的同时尽可能减少硬件耗能，提高硬件效率。可作为轻量级密码算法的扩散层，适用于计算能力有限的环境。为了寻找XORs较少的MDS矩阵，学者们做了许多的工作[8–11]，利用一些特殊结构的矩阵如循环矩阵、Hadamard矩阵等来构造扩散矩阵。2016年，Sarkar等人[10]利用一种特殊结构矩阵Toeplitz矩阵构造了有限域$\mathbb{F}_{2^4}$和$\mathbb{F}_{2^8}$上的4×4MDS矩阵，XORs达到了当时的最优结果。2017年Jean等人在文献[11]中给出了一种新的XORs计算方法，新的计算方法不考虑使用临时寄存器的情况，这在实际应用时是更容易实现的，可以降低矩阵的XORs。利用新的XORs计算方法，文献[12]构造了XORs优于当时已知最优结果的多维度的MDS循环矩阵。

本文考虑利用Toeplitz矩阵以及新的XORs计算方法是否能进一步减少MDS矩阵的XORs。在对称密码算法中，最常用的是4 bit S盒和8 bit S盒，最常用扩散矩阵的维度是4，当矩阵维度较大时，计算复杂度会变得非常复杂。当S盒为4 bit时，两种XORs计算方法对有限域元素的最小XORs没有影响，因此本文主要研究8 bit S盒即在有限域$\mathbb{F}_{2^8}$上的扩散矩阵。同时由于计算能力的限制，本文主要研究了4×4 MDS Toeplitz矩阵，同时给出矩阵维度为5和6时的情况。在同一种XORs计算方法下，本文给出的有限域$\mathbb{F}_{2^8}$上的4×4MDS Toeplitz矩阵的XORs为20，优于已知最好结果24; 5×5MDS Toeplitz矩阵的XORs为40，与已知最优结果相等；6×6MDS Toeplitz矩阵的XORs为80，优于已知最好结果84。同时本文的结果全部优于传统XORs计算方法下的最优结果。

本文的结构安排如下：第2节给出了本文所涉及的符号表示及相关基础知识；第3节给出Toeplitz矩阵的介绍和相关性质，以及本文的构造结果；第4节给出了一个简短的总结。

2　基础知识

2.1　符号表示

XORs：异或操作次数；

$\mathbb{F}_p$：若p是素数，本文用$\mathbb{F}_p$表示有限域，本文考虑二元域，$p=2$；

$\mathbb{F}_{2^n}$: $\mathbb{F}_{2^n}\cong\mathbb{F}_2[x]/(q)$, $q\in\mathbb{F}_2(x)$是一个n次不可约多项式；

$\boldsymbol{E}_{i,j}$：第i行的第j个元素为1，其余均为0，其中$i,j\in\{1,2,\cdots,n\}$；

$\boldsymbol{I}_n$：n维单位矩阵；

$\mathrm{wt}(\boldsymbol{A})$：矩阵$\boldsymbol{A}$的非0元素的个数；

$\mathrm{wt}_{\oplus}(\boldsymbol{A})$：矩阵$\boldsymbol{A}$的XORs；

$\mathcal{B}_{\mathrm{d}}(\boldsymbol{L})$：矩阵$\boldsymbol{L}$的差分分支数；

$\mathcal{B}_{\mathrm{l}}(\boldsymbol{L})$：矩阵$\boldsymbol{L}$的线性分支数；

$\omega_{\mathrm{b}}(\boldsymbol{X})$：向量$\boldsymbol{X}$中非0元素的个数。

2.2　MDS矩阵

定义1　矩阵$\boldsymbol{L}$是$\mathbb{F}_{2^m}$上的$n\times n$矩阵，$\boldsymbol{L}$的差分分支数定义为$\mathcal{B}_{\mathrm{d}}(\boldsymbol{L})=\min\{\omega_{\mathrm{b}}(X)+\omega_{\mathrm{b}}(\boldsymbol{L}(X))\,|\,X=(x_1,x_2,\cdots,x_n)\in\mathbb{F}_{2^m}^n, X\neq 0\}$；$\boldsymbol{L}$的线性分支数定义为$\mathcal{B}_{\mathrm{l}}(\boldsymbol{L})=\min\left\{\omega_{\mathrm{b}}(X)+\omega_{\mathrm{b}}\left(\boldsymbol{L}^{\mathrm{T}}(X)\right)|X=(x_1,\right.$

$x_2,\cdots,x_n)\in\mathbb{F}_{2^m}^n, X\neq 0\}$。当$B_{\mathrm{d}}(\boldsymbol{L})=B_1(\boldsymbol{L})=n+1$时，矩阵$\boldsymbol{L}$的分支数达到最大，称为MDS矩阵。

验证一个矩阵是否为MDS矩阵时，需要验证其是否满足引理1。

引理1[13] $\boldsymbol{L}$是一个n维的MDS矩阵，n是一个正整数且$n\geq 2$。则$\boldsymbol{L}$是一个MDS矩阵的充要条件是：对任意的$1\leq g\leq n$，矩阵$\boldsymbol{L}$的每一个$g\times g$子矩阵均为非奇异。

2.3 异或操作次数(XORs)

定义2 有限域内的元素$\alpha\in\mathbb{F}_{2^m}$，其与有限域内的任意一个元素$b\in\mathbb{F}_{2^m}$相乘所需的异或操作的次数即为$\alpha$的XORs，记为$\mathrm{XOR}(\alpha)$。

统计一个扩散矩阵的XORs需将矩阵内所有元素的XORs相加，$\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}\gamma_{ij}+(\ell_i-1)\cdot m\right)=C(M)+\sum_{i=0}^{n-1}(\ell_i-1)\cdot m$，其中，$\gamma_{ij}$是矩阵第$i$行第$j$个元素的XORs，$\ell_i$是该行非0元素的个数，$C(M)$是矩阵所有元素的XORs之和。为了方便计算，本文只考虑$C(M)$的值。

2.3.1 有限域元素XORs的性质

左乘有限域$\mathbb{F}_{2^m}$内的一个元素α，可以用左乘一个可逆矩阵$\boldsymbol{M}_{\alpha,B}$来表示，有限域元素的XORs定义在文献[7]和文献[14]中已经详细介绍过，文献[7]给出的XORs定义为，一个m维可逆矩阵$\boldsymbol{A}$若可以表示成一个有t个多余非0元素的置换矩阵，即$\boldsymbol{A}=\boldsymbol{P}+\sum_{k=1}^{t}\boldsymbol{E}_{i_k,j_k}$，其中$\boldsymbol{P}$为一个置换矩阵，$\boldsymbol{E}_{i_k,j_k}$为第$i_k$行第$j_k$列为1，其余元素为0的矩阵，则$wt(\boldsymbol{A})=m+t$，即矩阵$\boldsymbol{A}$的XORs为$t$。虽然这种结构的矩阵在应用时最多有$t$次异或运算，但该结构未包含所有的最多可以通过$t$次异或运算实现的矩阵。下面给出本文所用的能包含上述情况的XORs的定义。这个改进的定义在文献[13]中第1次被提出。

定义3[13] 若可逆矩阵$\boldsymbol{A}$可以被表示为$\boldsymbol{A}=\boldsymbol{P}\prod_{k=1}^{t}(\boldsymbol{I}+\boldsymbol{E}_{i_k,j_k}), i_k\neq j_k k$, t是使得其成立的最小值，则可逆矩阵$\boldsymbol{A}$的XORs为t，记为$\mathrm{wt}_{\oplus}(\boldsymbol{A})=t$。

在置换等价类下，矩阵的XORs是不变的，若$\boldsymbol{A}\sim_{\pi}\boldsymbol{A}'$，则$\mathrm{wt}_{\oplus}(\boldsymbol{A})=\mathrm{wt}_{\oplus}(\boldsymbol{A}')$，矩阵的逆的XORs也是不变的，且满足引理2。

引理2[12] 若$\mathrm{XOR}(\alpha)=t$，则$\mathrm{XOR}(\alpha^s)\leq|s\cdot t|$。

根据引理2，在已知α的XORs的情况下，很容易得知$\{\alpha^{-1},\alpha^2,\alpha^{-2},\cdots\}$等元素的XORs，为方便计算矩阵的XORs，本文利用元素$\{1,\alpha,\alpha^{-1},\alpha^2,\alpha^{-2},\cdots\}$等来构造矩阵。为了构造XORs较少的矩阵，就需要利用XORs较少的有限域元素α。

2.3.2 具有最优XORs的有限域元素

本文面临的一个问题是寻找在应用时具有最少的XORs的有限域元素。$\alpha=1$时，因为对于任意的基B, $M_{1,\mathrm{B}}=\mathbf{I}_n$，因此XORs为0。

引理3[12] 令$\alpha\in\mathbb{F}_{2^m}$，对于一组基B，存在一个矩阵$\boldsymbol{A}=\boldsymbol{M}_{\alpha,\mathrm{B}}$满足$\mathrm{wt}_{\oplus}(\boldsymbol{A})=1$当且仅当$m_\alpha$是一个$m$次不可约3项式。

引理4[12] 若m_α是一个n次不可约5项式，则存在一组基B使得$\mathrm{wt}_{\oplus}(\boldsymbol{M}_{\alpha,\mathrm{B}})=2$，即$\mathrm{XOR}(\alpha)=2$。

在实际应用时最常用的是4 bit S盒和8 bit S盒，本文研究8 bit S盒即$m=8$的情况。在定义3给出的XORs定义下，$m=8$时有限域$\mathbb{F}_{2^8}$内存在元素α，其最小多项式为$x^8+x^6+x^5+x+1$，由引理4可知，α的XORs为2。

3 最优矩阵构造新结果

3.1 Toeplitz矩阵的定义及性质

定义4[12] 一个矩阵如果从左到右每一个下降对角线上的值是相等的，即该矩阵只由其第1行和第1列元素决定，则该矩阵称为Toeplitz矩阵。

下面举例给出一个$n\times n$Toeplitz矩阵

$$\boldsymbol{T}=\begin{bmatrix}a_0 & a_1 & a_2 & \cdots & a_{n-1}\\ a_{-1} & a_0 & a_1 & \cdots & a_{n-2}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ a_{-(n-1)} & a_{-(n-2)} & a_{-(n-3)} & \cdots & a_0\end{bmatrix}\tag{1}$$

Toeplitz矩阵只由其第1行和第1列元素决定，因此本文用$\mathrm{Toep}\left(a_0,a_1,\cdots,a_{-1},a_{-2},\cdots,a_{-(n-1)}\right)$来表示式(1)形式的Toeplitz矩阵。该矩阵也可以表示为$\boldsymbol{T}=[m_{i,j}], m_{i,j}=a_{j-i}$。根据Toeplitz矩阵的特殊结构，下面给出Toeplitz矩阵的一些性质，利用这些性质在搜索MDS矩阵时可以大大减少搜索复杂度。

定理1 假设$\boldsymbol{T}=\mathrm{Toep}\left(a_0,a_1,\cdots,a_{-1},a_{-2},\cdots,a_{-(n-1)}\right)$是式(1)形式的Toeplitz矩阵，若$a_i=a_{i+t}=a_{i+2t}$，且满足条件$i\geq-(n-1), i+2t\leq n-1, 1\leq t\leq n-1$，则$\boldsymbol{T}$不是MDS矩阵。

证明 给定一个矩阵$\boldsymbol{T}=\mathrm{Toep}\left(a_0,a_1,\cdots,a_{-1},a_{-2},\cdots,a_{-(n-1)}\right)$，存在$i,t$满足$i\geq-(n-1), i+2t\leq n-1, 1\leq t\leq n-1$，则$\boldsymbol{T}$中一定存在一个子矩阵$\begin{bmatrix}a_{i+t} & a_{i+2t}\\ a_i & a_{i+t}\end{bmatrix}$，因为$a_i=a_{i+t}=a_{i+2t}$，所以该子矩阵行列式为0，由引理1可知，$\boldsymbol{T}$一定不是MDS矩阵，定理得证。

利用定理1，在搜索MDS Toeplitz矩阵时可以排除很多候选矩阵，有利于降低复杂度。

引理5[15] 假设$\boldsymbol{T}=\mathrm{Toep}\left(a_0,a_1,\cdots,a_{-1},a_{-2},\cdots,a_{-(n-1)}\right)$是式(1)形式的Toeplitz矩阵，$\boldsymbol{T}$的每一个

$d\times d$ 子矩阵都等于$\boldsymbol{T}$的一个特定的$d\times d$子矩阵$\boldsymbol{T}_{\text{sub}}$，$\boldsymbol{T}_{\text{sub}}$满足如下条件：

(1) $\boldsymbol{T}_{\text{sub}}$的第1行元素属于$\boldsymbol{T}$的第1行元素；

(2) $\boldsymbol{T}_{\text{sub}}$的第1列元素属于$\boldsymbol{T}$的第1列元素。

由此可以计算出矩阵$\boldsymbol{T}=\text{Toep}\left(a_0,a_1,\cdots,a_{-1},a_{-2},\cdots,a_{-(n-1)}\right)$中不同的$d\times d$子矩阵的个数为$\begin{bmatrix}n-1\\d-1\end{bmatrix}^2+2\begin{bmatrix}n-1\\d-1\end{bmatrix}\begin{bmatrix}n-1\\d\end{bmatrix}=\begin{bmatrix}n-1\\d-1\end{bmatrix}^2\begin{bmatrix}2n-d\\d\end{bmatrix}$。因此，当$1\le d\le n$时，$\boldsymbol{T}$的所有维度不同子矩阵的个数为$\begin{bmatrix}2n-2\\n-1\end{bmatrix}+2\begin{bmatrix}2n-2\\n-2\end{bmatrix}$。由引理5可知，在验证矩阵$\boldsymbol{T}$是否为MDS矩阵时只需验证$\begin{bmatrix}2n-2\\n-1\end{bmatrix}+2\begin{bmatrix}2n-2\\n-2\end{bmatrix}$个子矩阵是否为非奇异的，结合上述定理1，可以大幅度降低搜索复杂度，有利于寻找高维度的MDS矩阵。

3.2 构造MDS Toeplitz矩阵

利用3.1节中的定理和引理，本节将构造有限域$\mathbb{F}_{2^8}$上的4×4, 5×5和6×6MDS Toeplitz矩阵。

3.2.1 MDS Toeplitz矩阵的构造

定理2 $\boldsymbol{T}_1(x)$是的有限域$\mathbb{F}_{2^m}$上的4×4Toeplitz矩阵

$$\boldsymbol{T}_1(x)=\begin{bmatrix}1&1&x^2&1\\x^{-1}&1&1&x^2\\x&x^{-1}&1&1\\x^2&x&x^{-1}&1\end{bmatrix}\tag{2}$$

若$x\in\mathbb{F}_{2^m}^*$，其最小多项式的次数≥5，且x不是多项式$X^5+X^4+X^3+X+1$的根，则$\boldsymbol{T}_1(x)$是MDS矩阵。

证明　因为x的最小多项式的次数>4，所以$x\ne1$。考虑矩阵$\boldsymbol{T}_1(x)$的所有不同的2×2子矩阵行列式的集Δ_2(Δ_3同理，矩阵$\boldsymbol{T}_1(x)$的所有不同的3×3子矩阵行列式集)

$$\Delta_2\left(\boldsymbol{T}_1(x)\right)=\begin{Bmatrix}(x+1)/x,1+x,(x^3+1)/x,1+x^2,\\1+x^4,\left(x^2+1\right)/x,1+x^3,x\left(1+x\right),\\\left(x^5+1\right)/x,\left(x^4+1\right)/x,\\\left(x^3+1\right)/x^2,\left(x^4+1\right)/x^2\end{Bmatrix}\tag{3}$$

$$\Delta_3\left(\boldsymbol{T}_1(x)\right)=\begin{Bmatrix}x^3+x,\left(x^5+x^2+x+1\right)/x^2,\\\left(x^6+x^3+x+1\right)/x,\left(x^4+1\right)/x,\\\left(x^6+x^3+x+1\right)/x^2,\left(x^5+x^4\right.\\\left.+x^3+1\right)/x,\left(x^5+x^4+x^3+x+1\right)/x,\\\left(x^6+x^5+x^4+x^3+x^2+1\right)/x^2,\\\left(x^2+1\right)/x,\left(x^5+x^4+x^3+1\right)/x,\\\left(x^4+1\right)/x^3\end{Bmatrix}\tag{4}$$

除$x^5+x^4+x^3+x+1$外，$\Delta_2\left(\boldsymbol{T}_1(x)\right)$和$\Delta_3\left(\boldsymbol{T}_1(x)\right)$中所有元素的分子都可以被因式分解为次数最大为4的$\mathbb{F}_2$上的不可约多项式，同时$\boldsymbol{T}_1(x)$的行列式为$\left(x^7+x^4+x^3+x\right)/x^3=(x+1)\left(x^5+x^4+x^3+x+1\right)/x^2$，因此，当$x$的最小多项式的次数$\ge5$，且$x$不是多项式$X^5+X^4+X^3+X+1$的根时，$\boldsymbol{T}_1(x)$是MDS矩阵。

实例1　根据结合2.3.2节以及定理2给出有限域$\mathbb{F}_{2^8}$上的$\boldsymbol{T}_1(\alpha)$，有限域元素α的最小多项式为$X^8+X^6+X^5+X+1$且XORs为2

$$\boldsymbol{T}_1(\alpha)=\begin{bmatrix}1&1&\alpha^2&1\\\alpha^{-1}&1&1&\alpha^2\\\alpha&\alpha^{-1}&1&1\\\alpha^2&\alpha&\alpha^{-1}&1\end{bmatrix}\tag{5}$$

因为α的最小多项式的次数为8满足定理2的条件，因此$\boldsymbol{T}_1(\alpha)$为MDS矩阵。元素$1,\alpha,\alpha^{-1},\alpha^2$的XORs分别为0, 2, 2, 4，矩阵中有2个α, 3个α^{-1}, 3个α^2，因此，矩阵$\boldsymbol{T}_1(\alpha)$中所有元素的XORs为$2\times2+3\times2+3\times4=22$。

在文献[12]中给出了相同XORs计算方法下最优的循环矩阵$\text{circ}\left(1,1,\alpha,\alpha^{-2}\right)$，其XORs为24。因此定理2给出的矩阵$\boldsymbol{T}_1(x)$已经优于已知最优结果。$\boldsymbol{T}_1(x)$为1的个数为8的MDS矩阵，下面给出1的个数为9的MDS矩阵。

定理3 $\boldsymbol{T}_2(x)$是的有限域$\mathbb{F}_{2^m}$上的4×4Toeplitz矩阵

$$\boldsymbol{T}_2(x)=\begin{bmatrix}1&1&x^2&x^{-1}\\x^{-1}&1&1&x^2\\1&x^{-1}&1&1\\x^2&1&x^{-1}&1\end{bmatrix}\tag{6}$$

若$x\in\mathbb{F}_{2^m}^*$的最小多项式的次数≥5，且x不是多项式$X^6+X^5+X^4+1$的根，则$\boldsymbol{T}_2(x)$是MDS矩阵。

证明　因为x的最小多项式的次数>4，所以$x\ne1$。考虑矩阵$\boldsymbol{T}_2(x)$的所有不同的2×2子矩阵行列式的集Δ_2(Δ_3同理，矩阵$\boldsymbol{T}_2(x)$的所有不同的3×3子矩阵行列式的集)

$$\Delta_2\left(\boldsymbol{T}_2(x)\right)=\begin{Bmatrix}(1+x)/x,1+x,1+x^2,x^2+x,\\x^4+x,\left(x^5+1\right)/x,1+x^3,\\\left(1+x^3\right)/x,\left(1+x^2\right)/x^2,\\\left(1+x^4\right)/x^2\end{Bmatrix}\tag{7}$$

$$\Delta_3(\boldsymbol{T}_2(x))=\left\{\begin{array}{l}x^2+1, x^2\left(x^2+1\right), x\left(x^2+1\right),\\ \left(x^6+x^4+x^3+x^2+x+1\right)/x^2,\\ \left(x^5+x^4+x^3+1\right)/x,\\ \left(x^5+x^4+x^3+1\right)/x^3,\\ \left(x^7+x^4+x+1\right)/x,\\ \left(x^5+x^2+x+1\right)/x^2,\\ \left(x^2+1\right)/x\end{array}\right\} \tag{8}$$

其中，$x^7+x^4+x+1=(x+1)\left(x^6+x^5+x^4+1\right)$，除$x^6+x^5+x^4+1$外，$\Delta_2(\boldsymbol{T}_2(x))$和$\Delta_3(\boldsymbol{T}_2(x))$中所有元素的分子都可以被因式分解为次数最大为4的$\mathbb{F}_2$上的不可约多项式，同时$\boldsymbol{T}_2(x)$的行列式为$\left(x^6+x^5+x^4+x^2+x+1\right)/x=\left(x^2+x+1\right)\left(x^4+1\right)/x$，因此，若$x$的最小多项式的次数$\geq 5$，且$x$不是多项式$X^6+X^5+X^4+1$的根，则$\boldsymbol{T}_2(x)$是MDS矩阵。

实例2 根据定理3构造有限域$\mathbb{F}_{2^8}$上的MDS矩阵并计算其XORs，与实例1中的有限域元素α相同，下面给出$\boldsymbol{T}_2(x)$的实例如式(9)所示

$$\boldsymbol{T}_2(\alpha)=\left[\begin{array}{cccc}1 & 1 & \alpha^2 & \alpha^{-1}\\ \alpha^{-1} & 1 & 1 & \alpha^2\\ 1 & \alpha^{-1} & 1 & 1\\ \alpha^2 & 1 & \alpha^{-1} & 1\end{array}\right] \tag{9}$$

$\boldsymbol{T}_2(\alpha)$中所有元素的XORs为$4\times 2+3\times 4=20$。因为α的最小多项式的次数为8，满足定理3中的条件，因此$\boldsymbol{T}_2(\alpha)$是MDS矩阵且XORs优于实例1给出的矩阵，进一步降低了矩阵的XORs。

文献[9]指出，有限域的不可约多项式不同时，元素的XORs有可能不同，有限域内的不同元素α的XORs也不同。本文遍历有限域$\mathbb{F}_{2^8}$的所有不可约多项式以及所有元素，未发现更优结果，由此本文得到了有限域$\mathbb{F}_{2^8}$上4×4MDS矩阵XORs下界的一个改进结果。

3.2.2 其他维度MDS Toeplitz矩阵的构造

定理4 $\boldsymbol{T}_3(x)$是的有限域$\mathbb{F}_{2^m}$上的5×5Toeplitz矩阵

$$\boldsymbol{T}_3(x)=\left[\begin{array}{ccccc}1 & x^2 & 1 & x^{-1} & x^{-1}\\ x^{-1} & 1 & x^2 & 1 & x^{-1}\\ x^{-1} & x^{-1} & 1 & x^2 & 1\\ 1 & x^{-1} & x^{-1} & 1 & x^2\\ x^2 & 1 & x^{-1} & x^{-1} & 1\end{array}\right] \tag{10}$$

若$x\in\mathbb{F}_{2^m}^*$的最小多项式的次数≥ 5，且x不是多项式$X^5+X^3+X^2+X+1$的根，则$\boldsymbol{T}_3(x)$是MDS矩阵。

证明 因为x的最小多项式的次数>4，所以$x\neq 1$。考虑矩阵$\boldsymbol{T}_3(x)$的所有不同的2×2子矩阵行列式的集Δ_2(Δ_3, Δ_4同理)

$$\Delta_2(\boldsymbol{T}_3(x))=\left\{\begin{array}{l}(1+x)/x, (1+x)/x^2, 1+x,\\ 1+x^4, \left(x^2+1\right)/x,\\ \left(x^2+1\right)/x^2, \left(1+x^3\right)/x,\\ \left(1+x^6\right)/x^2, \left(1+x^4\right)/x^2\end{array}\right\} \tag{11}$$

$$\Delta_3(\boldsymbol{T}_3(x))=\left\{\begin{array}{l}\left(x^5+x^2+x+1\right)/x^2, \left(x^6+x^5\right.\\ \left.+x^3+1\right)/x^2, \left(x^7+x^2+x+1\right)/x^3,\\ \left(x^6+x^5+x^4+x^2+x+1\right)/x^3,\\ \left(x^5+x^4+x^3+1\right)/x^3,\\ \left(x^4+1\right)/x^3, x^2+1,\\ 1+x^6, x^6+x^2\end{array}\right\} \tag{12}$$

$$\Delta_4(\boldsymbol{T}_3(x))=\left\{\left(x^7+x\right)/x^4, x^3+x^2,\left(x^5+x^3+x^2+x+1\right)/x^4\right\} \tag{13}$$

除了$x^5+x^3+x^2+x+1$外，$\Delta_2(\boldsymbol{T}_3(x))$, $\Delta_3(\boldsymbol{T}_3(x))$和$\Delta_4(\boldsymbol{T}_3(x))$中所有元素的分子都可以被因式分解为次数最大为4的$\mathbb{F}_2$上的不可约多项式，同时$\det(\boldsymbol{T}_3(x))=\left(x^5+x^3+x^2+x+1\right)/x^2$，因此，若$x$的最小多项式的次数$\geq 5$，且$x$不是多项式$X^5+X^3+X^2+X+1$的根，则$\boldsymbol{T}_3(x)$是MDS矩阵。

实例3 根据定理4给出有限域$\mathbb{F}_{2^8}$上的5×5 MDS矩阵，与实例1, 2选择的有限域元素α相同，下面给出$\boldsymbol{T}_3(x)$的实例矩阵如式(14)所示

$$\boldsymbol{T}_3(\alpha)=\left[\begin{array}{ccccc}1 & \alpha^2 & 1 & \alpha^{-1} & \alpha^{-1}\\ \alpha^{-1} & 1 & \alpha^2 & 1 & \alpha^{-1}\\ \alpha^{-1} & \alpha^{-1} & 1 & \alpha^2 & 1\\ 1 & \alpha^{-1} & \alpha^{-1} & 1 & \alpha^2\\ \alpha^2 & 1 & \alpha^{-1} & \alpha^{-1} & 1\end{array}\right] \tag{14}$$

α的最小多项式的次数为8，满足定理4中的条件，因此$\boldsymbol{T}_3(\alpha)$是MDS矩阵。$\boldsymbol{T}_3(\alpha)$有10个α^{-1}，5个α^{-2}，因此在有限域$\mathbb{F}_{2^8}$内，矩阵$\boldsymbol{T}_3(\alpha)$所有元素XORs之和的最小值为$10\times 2+5\times 4=40$，与文献[12]给出的5×5MDS循环矩阵的XORs最小值相同，结果没有改进。

定理5 $\boldsymbol{T}_4(x)$是的有限域$\mathbb{F}_{2^m}$上的6×6Toeplitz矩阵

$$\boldsymbol{T}_4(x)=\left[\begin{array}{cccccc}1 & x & x & 1 & x^{-2} & x^2\\ x^{-2} & 1 & x & x & 1 & x^{-2}\\ x^2 & x^{-2} & 1 & x & x & 1\\ x^{-2} & x^2 & x^{-2} & 1 & x & x\\ 1 & x^{-2} & x^2 & x^{-2} & 1 & x\\ x & 1 & x^{-2} & x^2 & x^{-2} & 1\end{array}\right] \tag{15}$$

若$x\in\mathbb{F}_{2^m}^*$的最小多项式的次数≥ 5，且x不是多项式$X^5+X^3+X^2+X+1$与X^6+X^2+X+1的根则$\boldsymbol{T}_4(x)$是MDS矩阵。

证明过程与定理2, 3, 4相似，简略。

$\boldsymbol{T}_4(x)$有10个x, 10个x^{-2}, 5个x^2，选择与之前实例相同的有限域元素α, α的最小多项式次数为8，满足定理5的条件，因此$\boldsymbol{T}_4(\alpha)$是MDS矩阵。有限域$\mathbb{F}_{2^8}$内，矩阵$\boldsymbol{T}_4(\alpha)$所有元素XORs之和的最小值为$10\times 2+10\times 4+5\times 4=80$，优于文献[12]给出的$6\times 6$MDS循环矩阵的XORs最小值84，得到改进的最优结果。

3.3 结果对比

表1给出了在有限域$\mathbb{F}_{2^8}$上，本文构造结果与已知的一些结果的对比。因为矩阵XORs的计算公式为$C(\boldsymbol{M})+n\cdot(n-1)\cdot m$，对MDS矩阵，当$n$和$m$确定时，$n\cdot(n-1)\cdot m$不变，因此表1中只给出了$C(\boldsymbol{M})$，即矩阵所有元素XORs之和。

需要注意的是，文献[12]的XORs计算方法与本文一致，文献[12,14]使用的是传统异或数计算方法。由表1可以看到，在4×4和6×6MDS矩阵中，本文的构造结果优于已知最好结果，5×5MDS Toeplitz矩阵的XORs等于已知最优结果。

表 1　本文构造结果与已知结果对比

矩阵维度	不可约多项式	矩阵实例$\boldsymbol{M}$	$C(\boldsymbol{M})$	文献
4×4	$x^8+x^6+x^5+x+1$	$\mathrm{Toep}\left(1,1,x^2,1,x^{-1},x,x^2\right)$	20	本文
4×4	$x^8+x^6+x^5+x+1$	$\mathrm{Circ}\left(1,1,x,x^{-2}\right)$	24	文献[12]
4×4	$x^8+x^7+x^6+x+1$	$\mathrm{Toep}\left(1,1,x,x^{-1},x^{-2},1,x^{-1}\right)$	27	文献[12]
4×4	$x^8+x^7+x^6+x+1$	$\mathrm{Left-Circ}\left(1,1,x,x^{-2}\right)$	32	文献[14]
4×4	$x^8+x^7+x^6+x+1$	$\mathrm{Had}\left(1,x,x^2,x^{-2}\right)$	52	文献[12]
5×5	$x^8+x^6+x^5+x+1$	$\mathrm{Toep}\left(1,x^2,1,x^{-1},x^{-1},x^{-1},x^{-1},1,x^2\right)$	40	本文
5×5	$x^8+x^6+x^5+x+1$	$\mathrm{Circ}\left(1,1,x,x^{-2},x\right)$	40	文献[12]
5×5	$x^8+x^7+x^6+x+1$	$\mathrm{Left-Circ}\left(1,1,x,x^{-2},x\right)$	55	文献[14]
6×6	$x^8+x^6+x^5+x+1$	$\mathrm{Toep}\left(1,x,x,1,x^{-2},x^2,x^{-2},x^2,x^{-2},1,x\right)$	80	本文
6×6	$x^8+x^6+x^5+x+1$	$\mathrm{Circ}\left(1,x,x^{-1},x^{-2},1,x^3\right)$	84	文献[12]
6×6	$x^8+x^7+x^6+x+1$	$\mathrm{Left-Circ}\left(1,x,x^{-1},x^{-2},1,x^3\right)$	108	文献[14]

4　结束语

本文从硬件效率较高的Toeplitz矩阵出发，利用不考虑临时寄存器的XORs计算方法，构造了XORs最少的轻量级MDS矩阵。选择XORs较少的有限域元素，在有限域$\mathbb{F}_{2^8}$上，构造了XORs为20的4×4 MDS Toeplitz矩阵和XORs为80的6×6MDS Toeplitz矩阵，分别优于已知最优XORs结果24和84。同时给出了XORs为40的5×5MDS Toeplitz矩阵，与已知最优XORs结果相等。根据MDS矩阵的性质以及Toeplitz矩阵的结构特点，给出了若Toeplitz矩阵是MDS矩阵，其矩阵元素所需满足的约束条件，利用该条件可以减少矩阵搜索的计算复杂度，有利于对高纬度MDS矩阵进行搜索。Toeplitz矩阵结构简单，便于硬件实现，因此具有最小XORs的MDS Toeplitz矩阵硬件效率较高，适合作为轻量级扩散矩阵，对轻量级密码算法的设计具有现实意义。同时如何利用其它类型特殊矩阵的性质来构造效率更高、维度更大的MDS扩散矩阵还需要进一步的研究与实验。

参 考 文 献

[1] BIHAM E and SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. *Journal of Cryptology*, 1991, 4(1): 3–72. doi: 10.1007/BF00630563.

[2] MATSUI M. Linear cryptanalysis method for DES cipher[C]. Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, 1993: 386–397.

[3] SHIRAI T, SHIBUTANI K, AKISHITA T, *et al*. The 128-bit blockcipher CLEFIA (extended abstract)[C]. The 14th International Workshop on Fast Software Encryption, Luxembourg, Luxembourg, 2007: 181–195. doi: 10.1007/978-3-540-74619-5_12.

[4] BOGDANOV A, KNUDSEN L R, LEANDER G, *et al*. PRESENT: An ultra-lightweight block cipher[C]. The 9th International Workshop on Cryptographic Hardware and Embedded Systems, Vienna, Austria, 2007: 450–466. doi: 10.1007/978-3-540-74735-2_31.

[5] GUO Jian, PEYRIN T, POSCHMANN A, *et al*. The LED block cipher[C]. The 13th International Workshop on Cryptographic Hardware and Embedded Systems, Nara, Japan, 2011: 326–341. doi: 10.1007/978-3-642-23951-9_22.

[6] YANG Gangqiang, ZHU Bo, SUDER V, *et al*. The SIMECK family of lightweight block ciphers[C]. The 17th International Workshop on Cryptographic Hardware and Embedded Systems, Saint-Malo, France, 2015: 307–329. doi: 10.1007/978-3-662-48324-4_16.

[7] SIM S M, KHOO K, OGGIER F, *et al*. Lightweight MDS involution matrices[C]. The 22nd International Workshop on Fast Software Encryption, Istanbul, Turkey, 2015: 471–493. doi: 10.1007/978-3-662-48116-5_23.

[8] LIU Meicheng and SIM S M. Lightweight MDS generalized circulant matrices[C]. The 23rd International Conference on Fast Software Encryption, Bochum, Germany, 2016: 101–120. doi: 10.1007/978-3-662-52993-5_6.

[9] LI Yongqiang and WANG Mingsheng. On the construction of lightweight circulant involutory MDS matrices[C]. The 23rd International Conference on Fast Software Encryption, Bochum, Germany, 2016: 121–139. doi: 10.1007/978-3-662-52993-5_7.

[10] SARKAR S and SYED H. Lightweight diffusion layer: Importance of Toeplitz matrices[J]. *IACR Transactions on Symmetric Cryptology*, 2016, 2016(1): 95–113. doi: 10.13154/tosc.v2016.i1.95-113.

[11] JEAN J, PEYRIN T, SIM S M, *et al*. Optimizing implementations of lightweight building blocks[J]. *IACR Transactions on Symmetric Cryptology*, 2017, 2017(4): 130–168. doi: 10.13154/tosc.v2017.i4.130-168.

[12] BEIERLE C, KRANZ T, and LEANDER G. Lightweight multiplication in $GF(2^n)$ with applications to MDS matrices[C]. The 36th Annual International Cryptology Conference, Santa Barbara, USA, 2016: 625–653. doi: 10.1007/978-3-662-53018-4_23.

[13] SARKAR S and SYED H. Analysis of Toeplitz MDS matrices[C]. The 22nd Australasian Conference on Information Security and Privacy, Auckland, New Zealand, 2017: 3–18. doi: 10.1007/978-3-319-59870-3_1.

[14] KHOO K, PEYRIN T, POSCHMANN A Y, *et al*. FOAM: Searching for hardware-optimal SPN structures and components with a fair comparison[C]. The 16th International Workshop on Cryptographic Hardware and Embedded Systems, Busan, South Korea, 2014: 433–450. doi: 10.1007/978-3-662-44709-3_24.

[15] JUNOD P and VAUDENAY S. Perfect diffusion primitives for block ciphers[C]. The 11th International Workshop on Selected Areas in Cryptography, Waterloo, Canada, 2004: 84–99. doi: 10.1007/978-3-540-30564-4_6.

陈少真：女，1967年生，教授，研究方向为密码学信息安全.

张怡帆：女，1993年生，硕士生，研究方向为信息安全.

任炯炯：男，1994年生，博士生，研究方向为信息安全.