International Journal of Digital Crime and Forensics
Volume 11 • Issue 4 • October-December 2019

Applying Horner's Rule to Optimize Lightweight MDS Matrices

Jian Bai, Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China

Yao Sun, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Ting Li, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Dingkang Wang, Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China

ABSTRACT

This article is concerned with the problem of constructing lightweight MDS matrices. The authors present a new construction of 4×4 MDS matrices over $GL(F_2, m)$ for any integer m. They give sufficient and necessary conditions to determine whether the construction is an MDS matrix. Further, for any even number $m \geq 4$, they construct lightweight MDS matrices in this structure. Applying Horner's rule to implement MDS matrices, the authors constructions need only $8+4\times3\times m$ XOR operations.

KEYWORDS

Diffusion Layer, Horner's Rule, Lightweight, MDS Matrix

1. INTRODUCTION

Diffusion and confusion are two fundamental properties that must be considered when designing symmetric-key ciphers (Shannon, 1949). These two properties are required for the security of the cipher. The diffusion layer is often obtained by a linear diffusion matrix. Matrices with higher branch number perform better to resist linear and differential attacks. The matrix with the maximum branch number is perfect for constructing diffusion layers and called a Maximal Distance Separable (MDS) matrix.

MDS matrices are widely used in many ciphers, including AES (Daemen &Rijmen, 2002), LED (Guo, Peyrin, & Poschmann, 2011) and SQUARE (Daemen, Knudsen, & Rijmen, 1997). When resources are limited, it is necessary to reduce the implementation costs when designing diffusion layers. For MDS matrices, the construction of lightweight MDS matrices becomes a hot topic, where lightweight MDS matrices means MDS matrices with small XOR counts.

The general method of constructing MDS matrices is based on the matrices with some specific structures. Since searching for all the MDS matrices is beyond the reach, when the dimension of the matrix increases. Circulant matrices and Hadamard matrices are preferred due to their limited number of different elements, which also leads to a smaller number of different minors. Circulant-like MDS matrices were constructed and the lightest MDS circulant-like matrices were found in (Junod & Vaudenay, 2005; Gupta & Ray, 2014). In 2014, Khoo et al. (Khoo, Peyrin, Poschmann, & Yap, 2014)

DOI: 10.4018/IJDCF.2019100106

introduced the metric XOR count that measures the implementation cost of a diffusion matrix. Based on this metric, there are a lot of works. Sarkar and Syed (Sarkar & Syed, 2016) gave theoretical constructions of Toeplitz MDS matrices and reported the minimum value of the XOR counts of 4×4 MDS matrices over F_{2^4} and F_{2^8}, respectively. Li et al. (Li, Bai, Sun, & Wang, 2016) reported the minimum value of the XOR counts of 4×4 MDS matrices over $\mathrm{GL}\left(\mathrm{F}_{2,} 4\right)$.

Another way for constructing lightweight MDS matrices is by recursive construction. This method was used in the design of PHOTON lightweight hash family (Guo, Peyrin, & Poschmann, 2011) and LED lightweight block cipher (Guo, Peyrin, Poschmann & Robshaw, 2011)for the first time. Sajadieh et al. (Sajadieh, Dakhilalian, Mala, & Sepehrdad, 2015) extended the recursive method by using linear transformations instead of multiplications of elements infinite fields. It helps to increase the choices of entries in MDS matrices. Then Wu et al. (Wu, Wang, & Wu, 2013) presented some extreme lightweight MDS matrices by using linear transformations with fewer XORs. Toh et al. (Toh, Teo, Khoo, & Sim, 2017) proposed a new class of serial-type matrices known as Diagonal Serial Invertible (DSI) matrices.

Recently, Beierle et al. (Beierle, Kranz, & Leander, 2016) and Jean et al. (Jean, Peyrin, Sim, & Tourteaux, 2017) proposed the s-metric to reduce the implementation cost of diffusion matrices. By finding a short linear straight-line program to the case of MDS matrices, Kranz et al. (Kranz, Leander, Stoffelen, & Wiemer, 2017) optimized the previous constructions globally. Their metric can be applied to any matrix and they found that MDS matrices of special types do not differ much for all randomized constructions.

Contributions. In this paper, we study the constructions of MDS matrices and present a new metric to reduce the implementation cost of MDS matrices.

First, we present a new structure to construct MDS matrices over $GL\left(F_2, m\right)$. Then we propose two conditions to construct MDS matrices and sufficient and necessary conditions under two different conditions are given.

Second, improve the implementing efficiency of diffusion matrices and reduce their XOR counts with the help of QinJiushao's method, also known as Horner's rule. We construct an MDS matrix with $8 + 4 \times 3 \times m$ XOR counts over $\mathrm{GL}\left(F_2, m\right)$, where $\mathrm{m} \geq 4$ and m is even.

Outline. We first give some necessary notations in Section 2. The way to construct 4×4 MDS matrices over $GL\left(F_2, m\right)$ is given in Section 3. In Section4, we apply Qin Jiushao's method to reduce the XOR counts. In this way, we can reduce XOR counts of the previous constructions. The conclusion comes in Section 5.

2. PRELIMINARIES

Let F_2 be the finite field of 2 elements and $\mathrm{F}_{2^{\mathrm{m}}}$ be an m-dimensional vector space over the field F_2. Denote by $\mathrm{F}_2^{\mathrm{m}\times\mathrm{m}}$ the set of all the $\mathrm{m}\times\mathrm{m}$ matrices over F_2. Let $\mathrm{E}_{\mathrm{i,j}}, \mathrm{i}, \mathrm{j} = 1,2,\ldots,\mathrm{n}$, be the matrix whose entries are all zeros except that the i-th row and the j-th column is 1. Denote by $\mathrm{M}_{\mathrm{i,j}}$ the entry at position $\left(\mathrm{i}, \mathrm{j}\right)$ of a matrix M. Denote by $GL\left(F_2, m\right)$ the set of all the $\mathrm{m}\times\mathrm{m}$ non-singular matrices with entries in the finite field F_2. If a linear basis of $\mathrm{F}_{2^{\mathrm{m}}}$ over F_2 is fixed, a linear permutation $\tilde{\mathrm{A}}_{\mathrm{a}} : \mathrm{F}_{2^{\mathrm{m}}} \rightarrow \mathrm{F}_{2^{\mathrm{m}}}$ can always be equivalently described as $\mathrm{X} \mapsto \mathrm{AX}$, where $\mathrm{A} \in \mathrm{GL}\left(\mathrm{F}_2, \mathrm{m}\right)$ and $\mathrm{X} \in \mathrm{F}_2^{\mathrm{m}}$.

Given a vector $\mathrm{X} = \left(\mathrm{x}_1, \mathrm{x}_2, \cdots, \mathrm{x}_{\mathrm{n}}\right) \in \left(\mathrm{F}_2^{\mathrm{m}}\right)^{\mathrm{n}}$, we can also view X as an element in the vector space $\mathrm{F}_2^{\mathrm{nm}}$. Here, X is viewed as a column vector throughout this paper. The bundle weight of X is

denoted by $\acute{E}_b(X)$ and defined as $\acute{E}_b(X) = \left|\{x_i : x_i \neq 0, 1 \leq i \leq n\}\right|$, where $|\cdot|$ means the size of a set.

For a matrix $L \in F_2^{nm \times nm}$, the branch number for m-bit words is defined as

$$B_m(L) := \min\{\acute{E}_b(X) + \acute{E}_b(LX) \mid X \in (F_2^m)^n\}.$$

It is easy to see, the upper bound of $B_m(L)$ is $n+1$, and a matrix achieved the bound is called an MDS matrix for m-bit words. In this paper, we focus on the case $n = 4$.

A matrix $L \in F_2^{nm \times nm}$ can be viewed as a $n \times n$ block matrix

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,2} \\ L_{2,1} & L_{1,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ L_{n,1} & L_{1,2} & \cdots & L_{m,n} \end{pmatrix}$$

where $L_{i,j} \in F_2^{m \times m}, 1 \leq i, j \leq n$.

Every linear diffusion is such a block matrix. Square block sub-matrices of L of order t means a $t \times t$ sub-matrices of L with entries in the set $\{L_{i,j} \mid 1 \leq i, j \leq n\}$. The following theorem given in (MacWilliams & Sloane, 1977) has shown that a matrix is an MDS matrix for m-bit words if and only if all its square block sub matrices are invertible. When talking about a block matrix is invertible, we view it as a matrix over the field F_2.

Theorem 1. Let $L \in F_2^{nm \times nm}$. Then L is an MDS matrix for m-bit words if and only if all square block sub-matrices of L of order t are of full rank for $1 \leq t \leq n$.

An addition in the field F_2 is called an XOR operation. For $A \in GL(F_2, m)$, we denote $\acute{E}(A)$ the number of nonzero entries in A. Denote $\#A$ the number of XOR operations that required to evaluate AX directly, where $X \in F_2^m$. That is to say, we need $\#A$ XOR operations to implement the linear permutation A over F_2^m. It is easy to know that $\#A = \acute{E}(A) - m$ and we call A has $\#A$ XOR operations. For space saving, we define a representation of sparse matrices over F_2. We extract the nonzero positions in each row. For example, for matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

the nonzero position 2 in the first row, 3 in the second row and 1,3 in the third row are extracted. Then we obtain the representation $[2, 3, [1, 3]]$. It is a matrix with 1 XOR operations.

The XOR counts of one linear diffusion matrix is the number of the XOR operations needed to be implemented. We can implement such a matrix L in a straightforward way. The XOR counts is denoted as

$$\mathrm{dXOR}\left(\mathrm{L}\right)=\sum_{\mathrm{i,j=1}}^{\mathrm{n}}\left(\#\,\mathrm{L}_{\mathrm{i,j}}\right)+\mathrm{n}\times\left(\mathrm{n}-1\right)\times\mathrm{m}\ .$$

In this paper, we focus on the MDS matrices for the case $\mathrm{n}=4$.

3. NEW CONSTRUCTIONS OF MDS MATRICES OVER GL(F2,M)

In this section, we present a method to construct MDS matrices over the general linear group $\mathrm{GL}\left(\mathrm{F}_2,\mathrm{m}\right)$. We obtain a simple sufficient and necessary condition to determine whether the construction is an MDS matrix.

The following lemma is useful to calculate minors of block matrices.

Lemma 1. Suppose $A,B,C\in GL\left(F_2,m\right)$ are $m\times m$ non-singular matrices over F_2. Then the following statements hold:

1. the determinant of matrix $\begin{pmatrix}I & A\\ B & C\end{pmatrix}$ is identical with that of matrix $BA+C$.
2. the determinant of matrix $\begin{pmatrix}A & I\\ B & C\end{pmatrix}$ is identical with that of matrix $CA+B$.
3. the determinant of matrix $\begin{pmatrix}A & B\\ I & C\end{pmatrix}$ is identical with that of matrix $AC+B$.
4. the determinant of matrix $\begin{pmatrix}A & B\\ C & I\end{pmatrix}$ is identical with that of matrix $AC+B$.
5. the determinant of matrix $\begin{pmatrix}A & B\\ B & A\end{pmatrix}$ is identical with that of matrix $\left(B+A\right)^2$.

Proof. The proof of the first four identities is similar. We only show the details of the first identity here. According to elementary linear algebra, we have

$$\begin{vmatrix}\mathrm{I} & \mathrm{A}\\ \mathrm{B} & \mathrm{C}\end{vmatrix}=\left|\begin{pmatrix}\mathrm{I} & 0\\ \mathrm{B} & \mathrm{I}\end{pmatrix}\cdot\begin{pmatrix}\mathrm{I} & \mathrm{A}\\ 0 & \mathrm{BA}+\mathrm{C}\end{pmatrix}\right|=\begin{vmatrix}\mathrm{I} & 0\\ \mathrm{B} & \mathrm{I}\end{vmatrix}\cdot\begin{vmatrix}\mathrm{I} & \mathrm{A}\\ 0 & \mathrm{BA}+\mathrm{C}\end{vmatrix}=\left|\mathrm{BA}+\mathrm{C}\right|.$$

Next, we prove the fifth identity.

$$\begin{vmatrix}\mathrm{A} & \mathrm{B}\\ \mathrm{B} & \mathrm{A}\end{vmatrix}=\left|\begin{pmatrix}\mathrm{I} & \mathrm{I}\\ 0 & \mathrm{I}\end{pmatrix}\cdot\begin{pmatrix}\mathrm{A}+\mathrm{B} & 0\\ \mathrm{B} & \mathrm{A}+\mathrm{B}\end{pmatrix}\cdot\begin{pmatrix}\mathrm{I} & \mathrm{I}\\ 0 & \mathrm{I}\end{pmatrix}\right|=\left|\left(\mathrm{A}+\mathrm{B}\right)^2\right|.$$

■

Now, we are able to prove the following theorem.

Theorem 2. Let $A,P\in GL\left(F_2,m\right),P=P^{-1}$ and $\#P=0$. Let I be the identity matrix in $GL\left(F_2,m\right)$, $f\left(x\right)$ be the minimal polynomial of A and

$$L := C\left(A,P\right) = \begin{pmatrix} I & P & A & APA^{-1} \\ \mathrm{APA}^{-1} & I & P & A \\ \mathrm{A} & APA^{-1} & I & P \\ \mathrm{P} & A & APA^{-1} & I \end{pmatrix}.$$

Then

1. If $\left(AP+I\right)^2 = 0$, then L is MDS $\Leftrightarrow f\left(x\right)$ is relatively prime to x^3+1 and x^3+x+1.
2. If $\left(A+P\right)^2 = 0$, then L is MDS $\Leftrightarrow f\left(x\right)$ is relatively prime to $x+1$ and x^3+x+1.

Proof. Since A and P are always non-commutative, we have to calculate all the minors of L by hand in order to verify that whether L is an MDS matrix.

Let $B = APA^{-1}$, then $B^2 = I$. Therefore, $\left|B\right| = \left|P\right| = \left|I\right| = 1$. Since $A \in GL\left(F_2, m\right)$ and $\left|A\right| \in F_2$, we have $\left|A\right| = \left|A^{-1}\right| = 1$. It is easy to see that $BA = APA^{-1}A = AP$.

$$L = \begin{pmatrix} I & P & A & B \\ \mathrm{B} & I & P & A \\ \mathrm{A} & B & I & P \\ \mathrm{P} & A & B & I \end{pmatrix}$$

has $\binom{4}{1}^2 + \binom{4}{2}^2 + \binom{4}{3}^2 + \binom{4}{4}^2 = 16+36+16+1 = 69$ minors in total. Since swapping rows (columns resp.) of a matrix over F_2 won't change the determinant of the matrix and the matrix L is circulant, the number of different minors which need to be computed is much less than 69. We list minors in terms of different orders below.

First, minors of order 1 are $\left|A\right|, \left|P\right|, \left|B\right|, \left|I\right|$ and they appear four times each. There are 16 minors of order 1 in total.

Second, minors of order 2

$$\begin{vmatrix} I & P \\ \mathrm{B} & I \end{vmatrix}, \begin{vmatrix} P & A \\ \mathrm{I} & P \end{vmatrix}, \begin{vmatrix} A & B \\ \mathrm{P} & A \end{vmatrix}, \begin{vmatrix} B & I \\ \mathrm{A} & B \end{vmatrix}, \begin{vmatrix} I & A \\ \mathrm{B} & P \end{vmatrix}, \begin{vmatrix} I & B \\ \mathrm{A} & P \end{vmatrix}, \begin{vmatrix} I & P \\ \mathrm{A} & B \end{vmatrix}, \begin{vmatrix} I & A \\ \mathrm{P} & B \end{vmatrix}$$

appear four times each and minors of order 2

$$\begin{vmatrix} I & A \\ \mathrm{A} & I \end{vmatrix}, \begin{vmatrix} B & P \\ \mathrm{P} & B \end{vmatrix}$$

appear twice each. There are 36 minors of order 2 in total.

Third, minors of order 3

$$\begin{vmatrix} I & P & A \\ \mathrm{B} & I & P \\ \mathrm{A} & B & I \end{vmatrix}, \begin{vmatrix} P & A & B \\ \mathrm{I} & P & A \\ \mathrm{B} & I & P \end{vmatrix}, \begin{vmatrix} B & I & P \\ \mathrm{A} & B & I \\ \mathrm{P} & A & B \end{vmatrix}, \begin{vmatrix} A & B & I \\ \mathrm{P} & A & B \\ \mathrm{I} & P & A \end{vmatrix}$$

appear four times each. There are 16 minors of order 3 in total.

At last, the unique minor of order 4 is $\left|L\right|$.

By Lemma 1, minors of 2 above are

$$\left|BP+I\right|,\left|A+I\right|,\left|APA+B\right|,\left|A+I\right|,\left|BA+P\right|,\left|AB+P\right|,\left|AP+B\right|,\left|PA+B\right|,\left|A+I\right|^2,\left|B+P\right|^2.$$

By factorizing these determinants, it is clear that all the minors of order 2 are non-zero if and only if $\left|AP+PA\right|,\left|A+I\right|,\left|AB+P\right|$ and $\left|PA+B\right|$ are all non-zero. Further, we reform $\left|AB+P\right|$ and $\left|PA+B\right|$ as

$$\left|AB+P\right| = \left|A^2PA^{-1}+P\right| = \left|A^2P+PA\right|\cdot\left|A^{-1}\right| = \left|A^2P+PA\right|$$

and

$$\left|PA+B\right| = \left|PA+APA^{-1}\right| = \left|PA^2+AP\right|\cdot\left|A^{-1}\right| = \left|PA^2+AP\right|,$$

respectively.

We will derive a simpler necessary and sufficient condition later under different assumptions.

First of all, we calculate the minors of order 3. With the help of Gaussian elimination, we could calculate the determinant of the following two square block sub-matrices. Add a multiple of second row of the matrix to the other two rows, then the second (first) entry in those two rows reduce to zero. Thus, we only need to calculate the determinant of a block matrix of order two.

$$\begin{vmatrix} I & P & A \\ \mathrm{B} & I & P \\ \mathrm{A} & B & I \end{vmatrix} = \begin{vmatrix} I & P & 0 \\ 0 & I & 0 \\ 0 & B & I \end{vmatrix}\cdot\begin{vmatrix} PB+I & 0 & A+I \\ \mathrm{B} & I & P \\ \mathrm{A}+I & 0 & BP+I \end{vmatrix} = \begin{vmatrix} PB+I & A+I \\ \mathrm{A}+I & BP+I \end{vmatrix},$$

$$\begin{vmatrix} P & A & B \\ \mathrm{I} & P & A \\ \mathrm{B} & I & P \end{vmatrix} = \begin{vmatrix} I & P & 0 \\ 0 & I & 0 \\ 0 & B & I \end{vmatrix}\cdot\begin{vmatrix} 0 & A+I & PA+B \\ \mathrm{I} & P & A \\ 0 & BP+I & BA+P \end{vmatrix} = \begin{vmatrix} A+I & PA+B \\ \mathrm{BP}+I & BA+P \end{vmatrix},$$

These two determinants can be computed further in specific conditions. Another two minors of order 3 can be computed directly without further conditions.

For the following block matrix, we use the second row to reduce the first entry in the other two rows to zero. Then the determinant of order three can be transformed into the determinant of order two. For the block matrix of order two, we use the second column to reduce the second entry in the first column to zero. Thus, we have

$$\begin{vmatrix} B & I & P \\ \mathrm{A} & B & I \\ \mathrm{P} & A & B \end{vmatrix} = \begin{vmatrix} I & P & 0 \\ 0 & I & 0 \\ 0 & B & I \end{vmatrix} \cdot \begin{vmatrix} PA+B & PB+I & 0 \\ \mathrm{A} & B & I \\ \mathrm{BA}+P & A+I & 0 \end{vmatrix}$$

$$= \begin{vmatrix} PA+B & PB+I \\ \mathrm{AP}+P & A+I \end{vmatrix}$$

$$= \begin{vmatrix} P & 0 \\ 0 & A+I \end{vmatrix} \cdot \begin{vmatrix} A+PB+BP+I & B+P \\ 0 & I \end{vmatrix} \cdot \begin{vmatrix} I & 0 \\ \mathrm{P} & I \end{vmatrix}$$

$= |P| \cdot |A+I| \cdot |A+I+BP+PB|$ (for both cases, $BP+PB = A^2 + A^{-2}$, which will be proved later)

$$= |A+I| \cdot |A+I+A^2+A^{-2}|$$

$$= |A+I|^2 \cdot |A^3+A+I| \cdot |A^{-2}|$$

$$= |A+I|^2 \cdot |A^3+A+I|.$$

For the following block matrix, we use the third row to reduce the first entry in the first two rows to zero. Then the determinant of order three can be transformed into the determinant of order two. For the block matrix of order two, we extract the common divisor $A+I$ of the first column. By lemma 1, we can calculate the determinant directly. Thus, we have

$$\begin{vmatrix} A & B & I \\ \mathrm{P} & A & B \\ \mathrm{I} & P & A \end{vmatrix} = \begin{vmatrix} I & 0 & A \\ 0 & I & P \\ 0 & 0 & I \end{vmatrix} \cdot \begin{vmatrix} 0 & AP+B & A^2+I \\ 0 & A+I & PA+B \\ \mathrm{I} & P & A \end{vmatrix} = \begin{vmatrix} AP+B & A^2+I \\ \mathrm{A}+I & PA+B \end{vmatrix}$$

$$= \begin{vmatrix} B & A^2+I \\ \mathrm{I} & PA+B \end{vmatrix} \cdot \begin{vmatrix} A+I & 0 \\ 0 & I \end{vmatrix} = |B(PA+B)+A^2+I| \cdot |A+I|$$

$$= |BPA+A^2| \cdot |A+I| = |A| \cdot |PA^{-1}P+I| \cdot |A| \cdot |A+I|$$

$$= |P| \cdot |A^{-1}| \cdot |A+I| \cdot |P| \cdot |A+I|$$

$$= |A+I|^2.$$

In the following, we calculate the minors under two assumptions respectively.

1. If $(AP+I)^2 = 0$, we have $APAP = I, AP = PA^{-1}, PA = A^{-1}P$. Then $B = APA^{-1} = A^2P = PA^{-2}$ and $BP+PB = A^2 + A^{-2}$.

   Then

$$\left|AP+PA\right|=\left|A+A^{-1}\right|=\left|A+I\right|^{2},$$

$$\left|AB+P\right|=\left|A^{2}P+PA\right|=\left|A^{3}+I\right|,$$

$$\left|PA+B\right|=\left|PA^{2}+AP\right|=\left|A^{2}+A^{-1}\right|=\left|A+I\right|\cdot\left|A^{2}+A+I\right|.$$

Then factors of minors of order 2 are $\left|A+I\right|$ and $\left|A^{2}+A+I\right|$. Since

$$\begin{vmatrix} I & P & A \\ \mathrm{B} & I & P \\ \mathrm{A} & B & I \end{vmatrix}=\begin{vmatrix} PB+I & A+I \\ \mathrm{A}+I & BP+I \end{vmatrix}=\begin{vmatrix} A^{-2}+I & A+I \\ \mathrm{A}+I & A^{2}+I \end{vmatrix}$$

$$=\begin{vmatrix} A^{-2} & 0 \\ 0 & A+I \end{vmatrix}\cdot\begin{vmatrix} A^{2}+I & I \\ \mathrm{I} & I \end{vmatrix}\cdot\begin{vmatrix} I & 0 \\ 0 & A+I \end{vmatrix}=\left|A+I\right|^{2}$$

and

$$\begin{vmatrix} P & A & B \\ \mathrm{I} & P & A \\ \mathrm{B} & I & P \end{vmatrix}=\begin{vmatrix} A+I & PA+B \\ \mathrm{BP}+I & BA+P \end{vmatrix}=\begin{vmatrix} A+I & A^{-1}P+A^{2}P \\ \mathrm{A}^{2}+I & AP+P \end{vmatrix}$$

$$=\begin{vmatrix} A^{-1} & 0 \\ 0 & A+I \end{vmatrix}\cdot\begin{vmatrix} A & A^{3}+I \\ \mathrm{I} & I \end{vmatrix}\cdot\begin{vmatrix} A+I & 0 \\ 0 & P \end{vmatrix}$$

$$=\left|A+I\right|\cdot\left|A^{3}+A+I\right|\cdot\left|A+I\right|$$

$$=\left|A+I\right|^{2}\cdot\left|A^{3}+A+I\right|,$$

factors of minors of order 3 are $\left|A+I\right|$ and $\left|A^{3}+A+I\right|$.

Next, we calculate the determinant of L.

$$\left|L\right|=\begin{vmatrix} I & P & A & B \\ \mathrm{B} & I & P & A \\ \mathrm{A} & B & I & P \\ \mathrm{P} & A & B & I \end{vmatrix}=\begin{vmatrix} I & 0 & 0 & 0 \\ \mathrm{B} & I & 0 & 0 \\ \mathrm{A} & 0 & I & 0 \\ \mathrm{P} & 0 & 0 & I \end{vmatrix}\cdot\begin{vmatrix} I & P & A & B \\ 0 & BP+I & AP+P & I+A \\ 0 & AP+B & A^{2}+I & A^{2}PA^{-1}+P \\ 0 & I+A & PA+B & PB+I \end{vmatrix}$$

$$=\begin{vmatrix} BP+I & AP+P & I+A \\ \mathrm{AP}+B & A^{2}+I & A^{2}PA^{-1}+P \\ \mathrm{A}+I & PA+B & PB+I \end{vmatrix}$$

$$= \begin{vmatrix} A^2+I & AP+P & A+I \\ \mathrm{A}^2P+AP & A^2+I & A^3P+P \\ \mathrm{A}+I & A^2P+A^{-1}P & A^{-2}+I \end{vmatrix}$$

$$= \begin{vmatrix} A+I & 0 & 0 \\ 0 & A+I & 0 \\ 0 & 0 & A+I \end{vmatrix} \cdot \begin{vmatrix} A+I & P & I \\ \mathrm{AP} & A+I & A^2P+AP+P \\ \mathrm{I} & AP+P+A^{-1}P & A^{-2}+A^{-1} \end{vmatrix}$$

$$= \left|A+I\right|^3 \cdot \begin{vmatrix} I & 0 & 0 \\ \mathrm{A}^2P+AP+P & I & 0 \\ \mathrm{A}^{-2}+A^{-1} & 0 & I \end{vmatrix} \cdot \begin{vmatrix} A+I & P & I \\ \left(A^2+A+A^{-1}\right)P & A^2 & 0 \\ \mathrm{A}^{-2} & \left(A+I+A^{-2}\right)P & 0 \end{vmatrix}$$

$$= \left|A+I\right|^3 \cdot \begin{vmatrix} \left(A^2+A+A^{-1}\right)P & A^2 \\ \mathrm{A}^{-2} & \left(A+I+A^{-2}\right)P \end{vmatrix}$$

$$= \left|A+I\right|^3 \cdot \begin{vmatrix} I & \left(A^2+A+A^{-1}\right)PA^2 \\ 0 & I \end{vmatrix} \cdot \begin{vmatrix} 0 & A^{-4}\left(A^2+A+I\right)\left(A^3+I\right) \\ \mathrm{A}^{-2} & \left(A+I+A^{-2}\right)P \end{vmatrix}$$

$$= \left|A+I\right|^4 \cdot \left|A\right|^{-6} \cdot \left|A^2+A+I\right|^2$$

$$= \left|A+I\right|^4 \cdot \left|A^2+A+I\right|^2.$$

After factorizing all the minors of L, we find that L is MDS $\Leftrightarrow A+I, A^2+A+I, A^3+A+I$ are all invertible $\Leftrightarrow f\left(x\right)$ is relatively prime to x^3+1, x^3+x+1.

2. If $\left(A+P\right)^2=0$, we have $A^2+AP+PA+I=0$. By multiplying P on the right side, we have

$$A^2P=\left(AP+PA+I\right)P=A+PAP+P=P\left(PA+AP+I\right)=PA^2.$$

Thus

$$AB=A^2PA^{-1}=PA^2A^{-1}=PA.$$

Since

$$B+P=APA^{-1}+P=\left(AP+PA\right)A^{-1}=\left(A^2+I\right)A^{-1}=A+A^{-1},$$

we have

$$PB + I = P\left(B + P\right) = P\left(A + A^{-1}\right)$$

and

$$BP + I = \left(B + P\right)P = \left(A + A^{-1}\right)P\,.$$

Since

$$A^{-2} + A^{-1}P + PA^{-1} + I = A^{-1}\left(I + PA + AP + A^{2}\right)A^{-1} = 0\,,$$

we obtain that

$$\begin{aligned} BP + PB &= \left(BP + I\right) + \left(PB + I\right) = P\left(A + A^{-1}\right) + \left(A + A^{-1}\right)P \\ &= \left(PA + AP\right) + \left(PA^{-1} + A^{-1}P\right) \\ &= \left(A^{2} + I\right) + \left(A^{-2} + I\right) \\ &= A^{2} + A^{-2}\,. \end{aligned}$$

Now we are ready to calculate all the minors of L .It is clear that

$$\left|AP + PA\right| = \left|A^{2} + I\right| = \left|A + I\right|^{2},$$
$$\left|AB + P\right| = \left|A^{2}P + PA\right| = \left|PA^{2} + PA\right| = \left|P\right|\cdot\left|A\right|\cdot\left|A + I\right| = \left|A + I\right|$$

and

$$\left|PA + B\right| = \left|PA^{2} + AP\right| = \left|A^{2}P + AP\right| = \left|A + I\right|\cdot\left|A\right|\cdot\left|P\right| = \left|A + I\right|.$$

Then there is a unique factor of minors of order 2, which is $\left|A + I\right|$.

The computation of minors of order 3 is much more complicated. We need to apply relations above repeatedly to obtain the determinant.

$$\begin{vmatrix} I & P & A \\ \mathrm{B} & I & P \\ \mathrm{A} & B & I \end{vmatrix} = \begin{vmatrix} PB + I & A + I \\ \mathrm{A} + I & BP + I \end{vmatrix} = \begin{vmatrix} P\left(A^{-1} + I\right) & A + I \\ \mathrm{I} & BP + I \end{vmatrix}\cdot\begin{vmatrix} A + I & 0 \\ 0 & I \end{vmatrix}$$

$$= \left|\left(PA^{-1} + P\right)\left(BP + I\right) + A + I\right|\cdot\left|A + I\right|$$

$$= \left|\left(A^{-1}P + PBP + PA^{-1} + P\right) + A + I\right|\cdot\left|A + I\right|$$

$$= \left|\left(A^{-1}P + PA^{-1} + I\right) + A + \left(PBP + P\right)\right| \cdot \left|A + I\right|$$
$$= \left|A^{-2} + A + P\left(BP + I\right)\right| \cdot \left|A + I\right|$$
$$= \left|A^{-2} + A + P\left(A + A^{-1}\right)P\right| \cdot \left|A + I\right|$$
$$= \left|A^{-2} + P\left(PA + AP\right) + PA^{-1}P\right| \cdot \left|A + I\right|$$
$$= \left|A^{-2} + P\left(A^2 + I\right) + PA^{-1}P\right| \cdot \left|A + I\right|$$
$$= \left|A^{-2}P\left(A + I\right)\left(P + A^3 + A^2\right)\right| \cdot \left|A + I\right|$$
$$= \left|P + A^3 + A^2\right| \cdot \left|A + I\right|^2.$$

By the equations obtained from the assumption, we have

$$\begin{vmatrix} P & A & B \\ \mathrm{I} & P & A \\ \mathrm{B} & I & P \end{vmatrix} = \begin{vmatrix} A+I & PA+B \\ \mathrm{BP}+I & BA+P \end{vmatrix} = \begin{vmatrix} A+I & 0 \\ 0 & I \end{vmatrix} \cdot \begin{vmatrix} I & B \\ \mathrm{BP}+I & BA+P \end{vmatrix}$$
$$= \left|A + I\right| \cdot \left|BPB + B + BA + P\right|$$
$$= \left|A + I\right| \cdot \left|PB + I + A + BP\right|$$
$$= \left|A + I\right| \cdot \left|A^2 + I + A + A^{-2}\right|$$
$$= \left|A + I\right|^2 \cdot \left|A^3 + A + I\right|,$$

Since

$$\left(P + A^3 + A^2\right)^2 = A^6 + I + A^3P + PA^3 + A^4$$
$$= A^6 + I + A^2\left(AP + PA\right) + A^4$$
$$= A^6 + I + A^2\left(A^2 + I\right) + A^4$$
$$= \left(A^3 + A + I\right)^2,$$

we have

$$\left|P + A^3 + A^2\right| = \left|A^3 + A + I\right|.$$

Therefore, factors of minors of order 3 are $|A + I$ and $\left|A^3 + A + I\right|$.
Finally, we only need to compute the determinant of the matrix L.

$$\left|L\right| = \begin{vmatrix} I & P & A & B \\ \mathrm{B} & I & P & A \\ \mathrm{A} & B & I & P \\ \mathrm{P} & A & B & I \end{vmatrix} = \begin{vmatrix} I & P & A & B \\ \mathrm{I} & I & P & A \\ \mathrm{I} & B & I & P \\ \mathrm{I} & A & B & I \end{vmatrix} \cdot \begin{vmatrix} I+P+A+B & 0 & 0 & 0 \\ \mathrm{I} & I & 0 & 0 \\ \mathrm{I} & 0 & I & 0 \\ \mathrm{I} & 0 & 0 & I \end{vmatrix}$$

$$= \begin{vmatrix} I & 0 & 0 & 0 \\ \mathrm{I} & I & 0 & 0 \\ \mathrm{I} & 0 & I & 0 \\ \mathrm{I} & 0 & 0 & I \end{vmatrix} \cdot \begin{vmatrix} I & P & A & APA^{-1} \\ 0 & P+I & A+P & P+A^{-1} \\ 0 & A+A^{-1} & A+I & A+A^{-1} \\ 0 & P+A & P+A^{-1} & APA^{-1}+I \end{vmatrix} \cdot \left|I+A^{-1}\right|$$

$$= \begin{vmatrix} I & 0 & 0 \\ 0 & I & 0 \\ \mathrm{I} & 0 & I \end{vmatrix} \cdot \begin{vmatrix} P+I & A+P & I+A^{-1} \\ \mathrm{A}+A^{-1} & A+I & 0 \\ \mathrm{I}+A & A+A^{-1} & 0 \end{vmatrix} \cdot \begin{vmatrix} I & 0 & I \\ 0 & I & 0 \\ 0 & 0 & I \end{vmatrix} \cdot \left|I+A^{-1}\right|$$

$$= \begin{vmatrix} I & 0 \\ \mathrm{I} & I \end{vmatrix} \cdot \begin{vmatrix} I+A^{-1} & A+I \\ 0 & A^{-1}+I \end{vmatrix} \cdot \begin{vmatrix} I & 0 \\ \mathrm{I} & I \end{vmatrix} \cdot \left|I+A^{-1}\right|^2$$

$$= \left|A+I\right|^4.$$

After factorizing all the minors of L, we find that L is MDS $\Leftrightarrow A+I, A^3+A+I$ are all invertible $\Leftrightarrow f\left(x\right)$ is relatively prime to $x+1, x^3+x+1$.

■

When m is large, it is difficult to determine whether there exists A, P meet the conditions in the above theorem. For even integer $m \geq 4$,we constructively prove the existence.

Theorem 3. If m is even and $m \geq 4$, there exists A, P, such that $\# A = 1$, $\left(A+P\right)^2 = 0$ and the minimal polynomial $f\left(x\right)$ of A is relatively prime to $x+1, x^3+x+1$.

Proof. Let $P = \sum_{i=1}^{\frac{m}{2}} \left(E_{2i-1,2i} + E_{2i,2i-1}\right)$, $A = \sum_{i=2}^{m} E_{i,i-1} + E_{1,m} + E_{2t+1,m}$ be the companion matrix of $x^m + x^{2t} + 1$ over F_2, where $1 < 2t < m$. Then $\left(A+P\right)^2 = 0$, since all the non-zero entries of $A+P$ are in the odd rows and the even columns. It is clear that $x^m + x^{2t} + 1$ and $x+1$ are relatively prime. Now we only need to prove that there exists t such that $x^m + x^{2t} + 1$ and $x^3 + x + 1$ are relatively prime. In fact, if $m = 4$, then $x^4 + x^2 + 1$ and $x^3 + x + 1$ are relatively prime. If $m \geq 6$, then either $x^m + x^2 + 1$ or $x^m + x^4 + 1$ is relatively to $x^3 + x + 1$, since $x^4 + x^2 = \left(x^m + x^2 + 1\right) + \left(x^m + x^4 + 1\right)$ and $x^3 + x + 1$ relatively prime.

■

Below we give some examples of MDS matrices which are constructed from Theorem 2.

Example 1. Example of P, A such that $\left(AP+I\right)^2 = 0$ and the minimal polynomial of A is relatively prime to x^3+1, x^3+x+1 with $\#A = 1$. Then $C\left(A,P\right)$ is an MDS matrix.

1. $m = 6$, $P = \left[6,5,4,3,2,1\right], A = \left[6,1,2,\left[3,6\right],4,5\right]$.

Example 2. Examples of P, A such that $\left(A+P\right)^2 = 0$ and the minimal polynomial of A is relatively prime to $x+1, x^3+x+1$ with $\#A = 1$. Then $C\left(A,P\right)$ is an MDS matrix.

1. $m = 4$, $P = \left[2,1,4,3\right], A = \left[4,1,\left[2,4\right],3\right]$.
2. $m = 8$, $P = \left[2,1,4,3,6,5,8,7\right], A = \left[8,1,\left[2,8\right],3,4,5,6,7\right]$.

4. APPLYING HORNER'S RULE TO REDUCE THE XOR COUNTS

Horner's method, also known as Qin Jiushao's algorithm, can be used to improve the efficiency, when calculating the values of polynomials. We could adapt it to reduce the practical XOR operations for implementing the diffusion layer.

For example, let $A, P \in GL\left(F_2, m\right)$ such that $\#A = \#A^{-1} = 1, \#P = 0, \#\left(APA^{-1}\right) \geq 2$. Then $dXOR$ of

$$x_1 + Px_2 + Ax_3 + APA^{-1}x_4, x_i \in F_2^m$$

is

$$\#I + \#P + \#A + \#APA^{-1} + 3\times m \geq 3 + 3m.$$

By Horner's rule, we can calculate the sum in a different way

$$x_1 + Px_2 + A\left(x_3 + PA^{-1}x_4\right).$$

If we calculate $x_3 + PA^{-1}x_4$ firstly and multiply the matrix A secondly, we only need $\#PA^{-1} + \#A + 3\times m = 2 + 3\times m$ XOR operations. In such way, the constructions in Theorem 3 only need $8 + 4\times 3\times m$ XOR operations to implement for any even number $m \geq 4$. In particular, when $m = 4$, our constructions need only $8 + 4\times 3\times 4$ XOR operations. However, the lightest ($dXOR$) 4×4 MDS matrices over $GL\left(F_{2,}4\right)$ has $10 + 4\times 3\times 4$ XOR counts, which is proved in (Li, Bai, Sun, Wang, & Lin, 2016). Therefore, Horner's method could successfully improve the lower bound of XOR count.

In fact, Horner' rule can also be used to reduce the XOR counts in the previous constructions. We compare our findings with the previous results in Table 1. In the table, s-XOR means the s-XOR metric in (Jean, Peyrin, Sim, & Tourteaux, 2017) and h-XOR means the XOR after applying Qin Jiushao's method (also known as Horner's rule) in this paper.

Table 1. Comparison Of 4 × 4 MDS matrices

Matrix		Implementation			Ref.
Field/Ring	Type	XOR	s-XOR	h-XOR	
F_{2^4} / $0x13$	Arbitrary	$13+4\cdot3\cdot4$	$10+4\cdot3\cdot4$	$13+4\cdot3\cdot4$	Jean et al., 2017
F_{2^4} / $0x19$	Toeplitz	$10+4\cdot3\cdot4$	$10+4\cdot3\cdot4$	$9+4\cdot3\cdot4$	Sarkar et al., 2016
$GL\left(4,F_2\right)$	Arbitrary	$10+4\cdot3\cdot4$	$10+4\cdot3\cdot4$	$9+4\cdot3\cdot4$	Li et al., 2016
$GL\left(4,F_2\right)$	Circulant	$12+4\cdot3\cdot4$	$12+4\cdot3\cdot4$	$12+4\cdot3\cdot4$	Li & Wang, 2016
F_{2^4}	Circulant	$16+4\cdot3\cdot4$	$12+4\cdot3\cdot4$	$16+4\cdot3\cdot4$	Beierle et al., 2016
$GL\left(4,F_2\right)$	Circulant	$12+4\cdot3\cdot4$	$12+4\cdot3\cdot4$	$8+4\cdot3\cdot4$	Example 2
$GL\left(8,F_2\right)$	Circulant	$12+4\cdot3\cdot8$	$12+4\cdot3\cdot8$	$12+4\cdot3\cdot8$	Li and Wang, 2016
$GL\left(8,F_2\right)$	Optimal	$10+4\cdot3\cdot8$	$10+4\cdot3\cdot8$	$10+4\cdot3\cdot8$	Li and Wang, 2016
F_{2^4} / $0x13$	Sub-field	$26+4\cdot3\cdot8$	$20+4\cdot3\cdot8$		Jean et al., 2017
$GL\left(8,F_2\right)$	Circulant	$12+4\cdot3\cdot8$	$12+4\cdot3\cdot8$	$8+4\cdot3\cdot8$	Example 2

5. CONCLUSION

In this paper, we present a method to construct lightweight MDS matrices over $GL\left(F_2,m\right)$. We use the idea of Horner's rule to optimize the implementation of MDS matrices. For any even integer $m\geq4$, we construct an MDS matrices with $8+4\cdot3\cdot m$ XOR counts and it is the lightest MDS matrix so far.

Finding the lightest MDS matrices based on Horner's rule is leaved as our future work.

REFERENCES

Beierle, C., Kranz, T., & Leander, G. (2016). Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices. In M. Robshaw & J. Katz (Eds.), *Advances in Cryptology – CRYPTO 2016. CRYPTO 2016* (pp. 625–663). Springer-Verlag. doi:10.1007/978-3-662-53018-4_23

Chand Gupta, K., & Ghosh Ray, I. (2014). On Constructions of Circulant MDS Matrices for Lightweight Cryptography. In X. Huang & J. Zhou (Eds.), *Information Security Practice and Experience. ISPEC 2014* (pp. 564–576). Cham: Springer. doi:10.1007/978-3-319-06320-1_41

Daemen, J., Knudsen, L. R., & Rijmen, V. (1997). The block cipher square. In *Proceedings of the 4th International Workshop on Fast Software Encryption, FSE '97* (pp. 149–165). London, UK: Springer-Verlag. doi:10.1007/BFb0052343

Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES - The Advanced Encryption Standard. Information security and cryptography*. Springer-Verlag. doi:10.1007/978-3-662-04722-4

Guo, J., Peyrin, T., & Poschmann, A. (2011). The PHOTON Family of Lightweight Hash Functions. In P. Rogaway (Ed.), *Advances in Cryptology – CRYPTO 2011. CRYPTO 2011* (pp. 222–239). Berlin Heidelberg, Germany: Springer-Verlag. doi:10.1007/978-3-642-22792-9_13

Guo, J., Peyrin, T., Poschmann, A., & Robshaw, M. (2011). The LED Block Cipher. In B. Preneel & T. Takagi (Eds.), *Cryptographic Hardware and Embedded Systems – CHES 2011. CHES 2011* (pp. 326–341). Springer-Verlag. doi:10.1007/978-3-642-23951-9_22

Jean, J., Peyrin, T., Sim, S., & Tourteaux, J. (2017). Optimizing implementations of lightweight building blocks. *IACR Transactions on Symmetric Cryptology,* (4), 130–168.

Junod, P., & Vaudenay, S. (2005). Perfect DiffusionPrimitives for Block Ciphers. In H. Handschuh & M. A. Hasan (Eds.), *Selected Areas in Cryptography. SAC 2004* (pp. 84–99). Springer-Verlag.

Khoo, K., Peyrin, T., Poschmann, A. Y., & Yap, H. (2014). Foam: Searching for hardware-optimal spn structures and components with a fair comparison. In L. Batina & M. Robshaw (Eds.), Lecture Notes in Computer Science: Vol. 8731. *Cryptographic Hardware and Embedded Systems – CHES 2014. CHES 2014* (pp. 433–450). Springer-Verlag.

Kranz, T., Leander, G., Stoffelen, K., and Wiemer, F. (2017). Shorter linear straight-line programs for MDS matrices. *IACR Transactions on Symmetric Cryptology,* (4), 188–211.

Li, T., & Bai, J. sun, Y., Wang, D., & Lin, D. (2016). The lightest 4×4 MDS matrices over $Gl(4, F2)$. *Cryptology ePrint Archive*. Retrieved from https://print.iacr.org/2016/686

Li, Y., & Wang, M. (2016). On the Construction of Lightweight Circulant Involutory MDS Matrices. In T. Peyrin (Ed.), *Fast Software Encryption. FSE 2016* (pp. 121–139). Springer-Verlag. doi:10.1007/978-3-662-52993-5_7

MacWilliams, F. J., & Sloane, N. J. A. (1977). *The theory of error-correcting codes*. North-Holland Publishing Company.

Sajadieh, M., Dakhilalian, M., Mala, H., & Sepehrdad, P. (2015). Efficient recursive diffusion layers for block ciphers and hash functions. *Journal of Cryptology*, *28*(2), 240–256. doi:10.1007/s00145-013-9163-8

Sarkar, S. & Syed, H. (2016). Lightweight diffusion layer: Importance of to eplitz matrices. *IACR Transactions Symmetric Cryptology,* (1), 95-113.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, *28*(4), 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x

Toh, D., Teo, J., Khoo, K., & Sim, S. M. (2017). Lightweight MDS serial-type matrices with minimal fixed xor count. In A. Joux, A. Nitaj, & T. Rachidi (Eds.), *Progress in Cryptology – AFRICACRYPT 2018. AFRICACRYPT 2018* (pp. 51–71). Cham: Springer. doi:10.1007/978-3-319-89339-6_4

Wu, S., Wang, M., & Wu, W. (2013). Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions. In L. R. Knudsen & H. Wu (Eds.), *Selected Areas in Cryptography. SAC 2012* (pp. 355–371). Springer-Verlag.