The Lightest 4x4 MDS Matrices over GL(4, $\mathbb{F}_2$)

Jian Bai, Dingkang Wang

KLMM, Academy of Mathematics and Systems Science, CAS, Beijing 100190, China

Abstract

MDS matrices are important parts for block ciphers. We searched the 4×4 MDS matrices over GL(4, $\mathbb{F}_2$), and found the lightest MDS matrices only have 10 XOR operations. Besides, all these lightest MDS matrices can be classified to 3 classes.

Keywords: MDS matrix, lightweight.

1. Introduction

MDS matrices are used as linear diffusion layer in symmetric cryptography, and provide better resistance to differential and linear attack. Lighter MDS matrices can lead to cheaper implementations both in softwares and hardwares. Many researchers are devoted to searching lighter MDS matrices in recent years [1, 2].

2. Notations

The notation $GL(m, S)$ denotes the set of all $m \times m$ non-singular matrices with entries in S, where S is generally a finite field. For any $a, b \in \mathbb{F}_2$, the operation $a + b$ is called a bit XOR operation. For a matrix $A \in GL(m, \mathbb{F}_2)$, we use $\#A$ to denote the number of XOR operations that is required to calculate $A \cdot x$ where $x \in \mathbb{F}_2^m$. It is easy to see

$$\#A = \sum_{i=1}^{m} (\omega(A[i]) - 1),$$

where $\omega(A[i])$ means the number of nonzero entries in the i-th row of A.

We consider the matrix having the following form:

$$L := (L_{i,j}) = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix},$$

where $L_{i,j} \in GL(m, \mathbb{F}_2)$ for $1 \leq i, j \leq n$. We denote $\#L := \sum_{i,j=1}^{n} (\#L_{i,j})$, and denote $\mathcal{M}(n, m)$ be the set of all matrices having the above form.

Square sub-matrices of L of order t means the following matrices

$$L(J,K) := (L_{j_l,k_p}, 1 \le l,p \le t)$$

where $J = [j_1, \cdots, j_t]$ and $K = [k_1, \cdots, k_t]$ are two sequences of length t, and $1 \le j_1 < \cdots < j_t \le n, 1 \le k_1 < \cdots < k_t \le n$.

Theorem 2.1. *Let $L \in \mathcal{M}(n,m)$. Then L is a MDS matrix if and only if all square sub-matrices of L of order t are of full rank for $1 \le t \le n$.*

3. Results

Li and Wang investigated the constructions of 4×4 lightweight MDS matrices with entries in the set of 4×4 non-singular matrices over $\mathbb{F}_2$ [2]. They found $\#L \ge 12$ and $\#L \ge 16$ for Circulant MDS matrices and Hadamard MDS matrices, respectively.

To find lighter MDS matrices, we searched all the lightweight matrices $L \in \mathcal{M}(4,4)$ such that $\#L \le 12$, and obtain the following theorem.

Theorem 3.1. *Let $L \in \mathcal{M}(4,4)$. If L is a MDS matrix, then $\#L \ge 10$.*

It takes about 1 days to verify that there is no MDS matrix L suth that $\#L \le 9$. We use less than 2 hours to find the first MDS matrix L with $\#L = 10$, and spend about one week to find out all MDS matrices with XOR number 10. Our platform is Intel i7-4790, 3.6 GHz with 16 GB memory, running Ubuntu 15.04.

We find all MDS matrices with XOR number 10 can be classified into 3 classes, by using the following equivalent relation.

Definition 3.2. *Consider a matrix $L = (L_{i,j}), 1 \le i,j \le n$ such that $L_{i,\sigma(j)} = I_m$ and $L_{i,k} = 0$ for $k \ne \sigma(j)$, where I_m is the $m \times m$ identity matrix over $\mathbb{F}_2$ and $\sigma(\cdot)$ is a permutation of $[1,2,\cdots,n]$. Let $\mathbb{P}$ be a set of all such L's.*

Let $\mathbb{Q}$ be a set of $Diag(L_1, L_2, \cdots, L_n)$, where $L_i \in GL(m, \mathbb{F}_2)$ and $\#L_i = 0$ for $i = 1,2,\cdots,n$.

For $M, N \in \mathcal{M}(n,m)$, we say M is equivalent to N, if there exists $P_1, P_2 \in \mathbb{P}, Q_1, Q_2 \in \mathbb{Q}$ such that $M = P_1 \cdot Q_1 \cdot N \cdot Q_2 \cdot P_2$.

In simple words, we say two MDS matrices, e.g. M and N, are equivalent, if M can be transformed to N by simply swapping rows and columns in some ways.

Theorem 3.3. *If L is a 4×4 MDS matrix over GL(4, $\mathbb{F}_2$) and $\#L = 10$, then L must be equivalent to an MDS matrix having one of the following three types. Let I be the 4×4 identity matrix over $\mathbb{F}_2$.*

1. $\begin{pmatrix} I & I & I & X \\ I & A & B & I \\ I & B & A & A \\ X & I & A & I \end{pmatrix}$, *where $AB = I$, $X = B^2$.*

2. $\begin{pmatrix} X & I & I & I \\ I & I & B & X \\ I & B & A & I \\ I & X & I & A \end{pmatrix}$, *where* $AB = I$, $X = A^2$.

3. $\begin{pmatrix} Y & I & I & I \\ I & I & A & B \\ I & A & I & X \\ I & B & X & I \end{pmatrix}$, *where* $A + B = X$.

Example 3.4. *We give one example for each type.*

Type1:
$$\begin{pmatrix}
1&0&0&0&1&0&0&0&1&0&0&0&0&1&1&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&1\\
0&0&1&0&0&0&1&0&0&0&1&0&1&0&0&0\\
0&0&0&1&0&0&0&1&0&0&0&1&1&1&0&0\\
1&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&1&0&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&1&1&0&1&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&1&1&0&0&0&0&1\\
1&0&0&0&0&0&0&1&0&1&0&0&0&1&0&0\\
0&1&0&0&1&0&0&0&0&0&1&0&0&0&1&0\\
0&0&1&0&0&1&0&0&0&0&1&1&0&0&1&1\\
0&0&0&1&0&1&1&0&1&0&0&0&1&0&0&0\\
0&1&1&0&1&0&0&0&0&1&0&0&1&0&0&0\\
0&0&0&1&0&1&0&0&0&0&1&0&0&1&0&0\\
1&0&0&0&0&0&1&0&0&0&1&1&0&0&1&0\\
1&1&0&0&0&0&0&1&1&0&0&0&0&0&0&1
\end{pmatrix}$$

Type2:
$$\begin{pmatrix}
0&1&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
1&0&1&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&1&0&0&1&0&0&0&1&0&0&0&1&0\\
0&1&1&0&0&0&0&1&0&0&0&1&0&0&0&1\\
1&0&0&0&1&0&0&0&1&0&0&1&0&1&0&0\\
0&1&0&0&0&1&0&0&0&0&1&0&1&0&1&0\\
0&0&1&0&0&0&1&0&1&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&1&0&1&0&0&0&1&1&0\\
1&0&0&0&1&0&0&1&0&0&1&0&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&0&1&0&0\\
0&0&1&0&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&0&1&0&0&1&0&1&0&0&0&0&1\\
1&0&0&0&0&1&0&0&1&0&0&0&0&0&1&0\\
0&1&0&0&1&0&1&0&0&1&0&0&0&0&0&1\\
0&0&1&0&0&0&0&1&0&0&1&0&0&1&0&0\\
0&0&0&1&0&1&1&0&0&0&0&1&1&0&1&0
\end{pmatrix}$$

Type3:

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

4. Reference

[1] S.M. Sim, K. Khoo, F. Oggier, and T. Peyrin. Lightweight MDS involution matrices. FSE 2015.

[2] Y. Li, M.S. Wang. On the construction of lightweight circulant involutory MDS matrices. FSE 2016.