SCIENCE CHINA
Information Sciences

• LETTER •

November 2018, Vol. 61 119102:1–119102:3
https://doi.org/10.1007/s11432-017-9320-8

The lightest 4×4 MDS matrices over $\mathrm{GL}(4, \mathbb{F}_2)$

Jian BAI[1,3†], Ting LI[2,4†], Yao SUN[2*], Dingkang WANG[1,3] & Dongdai LIN[2]

[1]*Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100190*, China;*
[2]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[3]*School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049*, China;*
[4]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049*, China*

Received 22 May 2017/Accepted 30 November 2017/Published online 12 September 2018

Citation Bai J, Li T, Sun Y, et al. The lightest 4×4 MDS matrices over $\mathrm{GL}(4, \mathbb{F}_2)$. Sci China Inf Sci, 2018, 61(11): 119102, https://doi.org/10.1007/s11432-017-9320-8

Dear editor,

We present an algorithm for searching MDS matrices without any prior structures. We find all the lightest 4×4 MDS matrices over $\mathrm{GL}(4, \mathbb{F}_2)$ that have 10 XOR-counts, including the Toeplitz MDS matrices presented in [1]. We classify all these lightest MDS matrices to 3 types, and give some sufficient and necessary conditions for these 3 types matrices for being MDS matrices. Using these conditions, we directly construct more 4×4 MDS matrices over $\mathrm{GL}(m, \mathbb{F}_2)$ with 10 XOR-counts for $m \geqslant 4$.

Preliminary. The matrices with the maximum branch numbers can be used to construct perfect diffusion layers. We call this kind of matrices maximal distance separable (MDS) matrices. Please note that all the matrices mentioned in this study are square matrices unless otherwise stated. The notation $\mathrm{GL}(m, S)$ 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 with 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 $1 \leqslant i, j \leqslant n$. We define $\mathcal{M}(n, m)$ as the set of all matrices that have the above form.

Generally, the XOR count reflects the number of all the XOR operations. Thus the total XOR operations of L is $\sum_{i,j=1}^{n} (\#L_{i,j}) + m \times (n-1) \times n$, where $m \times (n-1) \times n$ is fixed. For convenience, we define the XOR count of the matrix L: $\#L = \sum_{i,j=1}^{n} (\#L_{i,j})$. In this study, we say that a matrix have 10 XOR-counts if the XOR count of this matrix is 10.

Square sub-matrices of L of order t means the following matrices $L(J, K) := (L_{j_l, k_p}, 1 \leqslant l, p \leqslant t)$, where $J = [j_1, \ldots, j_t]$ and $K = [k_1, \ldots, k_t]$ are two sequences of length t, and $1 \leqslant j_1 < \cdots < j_t \leqslant n, 1 \leqslant k_1 < \cdots < k_t \leqslant n$.

The following two propositions are well known.

Proposition 1 (Theorem 1 in [2])**.** Let $L \in \mathcal{M}(n, m)$. Then L is an MDS matrix if and only if all square sub-matrices of L of order t are of full rank for $1 \leqslant t \leqslant n$.

* Corresponding author (email: sunyao@iie.ac.cn)
† Jian BAI and Ting LI have the same contributions to this work.

In order to speed up the searching of MDS matrices, we need to define a stronger equivalent relation between MDS matrices.

Definition 1. Consider a matrix $L = (L_{i,j}), 1 \leqslant i, j \leqslant n$ such that $L_{i,\sigma(i)} = I_m$ and $L_{i,j} = 0$ for $j \neq \sigma(i)$, where I_m is the $m \times m$ identity matrix over $\mathbb{F}_2$ and $\sigma(\cdot)$ is a permutation of $[1, 2, \ldots, n]$. Let $\mathbb{P}$ be a set of all such L's. Let $\mathbb{Q}$ be a set of $\mathrm{Diag}(L_1, L_2, \ldots, L_n)$, where $L_i \in GL(m, \mathbb{F}_2)$ and $\#L_i = 0$ for $i = 1, 2, \ldots, n$. 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 $M = P_1 \cdot Q_1 \cdot N \cdot Q_2 \cdot P_2$.

For any $P \in \mathbb{P}, Q = \mathrm{Diag}(L_1, L_2, \ldots, L_n) \in \mathbb{Q}$, where $P_{i,\sigma(i)} = I_m$ and $P_{i,j} = 0$ for $j \neq \sigma(i)$, it is easy to verify that $P \cdot Q = \mathrm{Diag}(L_{\sigma(1)}, L_{\sigma(2)}, \ldots, L_{\sigma(n)}) \cdot P$. Therefore, the relation in Definition 1 is an equivalent relation.

Proposition 2. For $M, N \in \mathcal{M}(n, m)$, if M is equivalent to N, we say M is an MDS matrix if and only if N is an MDS matrix.

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.

According to this equivalence, we define the row/column-minimal form of a matrix in $\mathrm{GL}(m, \mathbb{F}_2)$. Given $M \in GL(m, \mathbb{F}_2)$ and let r_i be the i-th row of M, $0 < i \leqslant m$, where r_i can be regarded as a binary number and the most significant bit is the left-most. Thus, the rows of M are comparable. Particularly, we say the i-th row is lighter than the j-th row, if the binary number of the i-th row is smaller. If $r_i \leqslant r_j$ for all i and j such that $0 < i < j \leqslant m$, we say that M is the row-minimal among all the equivalent matrices. Similarly, we can defined the column-minimal form, where the most significant bit is the top-most.

Main results. First, we describe the main idea of searching the lightest 4×4 MDS matrix over $\mathrm{GL}(4, \mathbb{F}_2)$. To illustrate the algorithm clearly, we give a detailed description of the algorithm for searching 2×2 MDS matrices.

A matrix in $\mathcal{M}(n, m)$ is partitioned into n^2 blocks, where each block is a matrix in $\mathrm{GL}(m, \mathbb{F}_2)$. For $M \in \mathcal{M}(2, 2)$, we write

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

if M are partitioned into these 4 blocks. The main idea is to loop over all matrices in $\mathrm{GL}(4, \mathbb{F}_2)$ for blocks A, B, C, and D. Then we check whether the 2×2 matrix is of full rank or not. To avoid repetitive search, for blocks A and C, we only need to consider the matrices in row-minimal form. As to block B, we only consider the matrices in column-minimal form. Proposition 2 shows that minimal form is enough to find all MDS matrices. Although we only consider the minimal form of blocks A, B, and C, all the 2×2 matrices are checked actually. When checking whether M is of full rank, we compute the rank of $D' = C \cdot A^{-1} \cdot B + D$ instead of M, which saves many computations since D' is smaller than M. The algorithm is shown as Algorithm 1.

Algorithm 1 The 2×2 searching algorithm

Output: The set of $2\times$ 2 MDS matrices $L \in \mathcal{M}(2, 4)$.

$L \Leftarrow \emptyset$;
for all every matrix $A \in GL(4, \mathbb{F}_2)$ **do**
  if A is not in row-minimal form **then**
    go to Step 2;
  end if
  for all every matrix $B \in GL(4, \mathbb{F}_2)$ **do**
    if B is not in column-minimal form **then**
      go to Step 6;
    end if
    for all every matrix $C \in GL(4, \mathbb{F}_2)$ **do**
      if C is not in row-minimal form **then**
        go to Step 10;
        for all every matrix $D \in GL(4, \mathbb{F}_2)$ **do**
          $D' \Leftarrow C \cdot A^{-1} \cdot B + D$;
          if D' is invertible **then**
            $L \Leftarrow L \cup \{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)\}$;
          end if
        end for
      end if
    end for
  end for
end for

The algorithm can be generalized to $n \times n$ MDS matrices directly. Here we take the 3×3 MDS matrices for example. We write

$$M = \begin{pmatrix} A & B & G \\ C & D & H \\ E & F & J \end{pmatrix},$$

where $M \in \mathcal{M}(3, 3)$. There are 9 for-loops in the algorithm corresponds to the blocks A–J. For each loop, the candidates are picked out from the singular matrices as well. Thus, steps of checking of sub-matrices of order 1 is omitted.

The sub-matrices of order 2 are constructed in the following sequence: $(A, B, C, D) \to (A, B, E, F) \to (C, D, E, F) \to (A, G, C, H) \to (B, G, D, H) \to (A, G, E, J) \to (B, G, F, J) \to (C, H, E, J) \to (D, H, F, J)$. To check whether the sub-matrices of order 3 are of full rank, we eliminate the blocks C and E to 0. Then we calculate the rank of

$$\begin{pmatrix} C \cdot A^{-1} \cdot B + D & C \cdot A^{-1} \cdot G + H \\ E \cdot A^{-1} \cdot B + F & E \cdot A^{-1} \cdot G + J \end{pmatrix}$$

and check if it is of full rank. After checking all the sub-matrices of orders 2 and 3, we can determine whether M is an MDS matrix. The method for searching 4×4 MDS matrices is similar and the loop order of blocks in M is

$$M = \begin{pmatrix} A & B & J & N \\ C & D & K & P \\ E & F & L & Q \\ G & H & M & R \end{pmatrix}.$$

Theorem 1. Let $L \in \mathcal{M}(4,4)$. If L is an MDS matrix, $\#L \geqslant 10$.

It takes about 1 days to verify that there is no MDS matrix L suth that $\#L \leqslant 9$. 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 10 XOR-counts. Our platform is Intel i7-4790, 3.6 GHz with 16 GB memory, running Ubuntu 15.04.

We find that all the MDS matrices with 10 XOR-counts can be classified into 3 types with respect to the equivalent relation defined in Definition 1. We summarize the structures of the lightest MDS matrices and obtain some of their properties via direct observations. In other words, the properties given below are only necessary conditions for matrices A, B, X, and Y.

Theorem 2. If L is a 4×4 MDS matrix over $\mathrm{GL}(4, \mathbb{F}_2)$ and $\#L = 10$, L must be equivalent to an MDS matrix that has 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 $AB = I$ and $X = B^2$.

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

(3) $\begin{pmatrix} Y & I & I & I \\ I & I & A & B \\ I & A & I & X \\ I & B & X & I \end{pmatrix}$, where $A + B = X$, $YA^2 = I$ and $A^2 = B^2 = X^2$.

We analyze these structures and give some sufficient and necessary conditions of the lightest 4×4 MDS matrices over $\mathrm{GL}(4, \mathbb{F}_2)$.

Theorem 3. For the matrices of Types (1) and (2) in Theorem 2 with $AB = I$ and $X = B^2$, they are MDS matrices if and only if

(1) $|B + I| \neq 0$,
(2) $|B^2 + B + I| \neq 0$,
(3) $|B^3 + B^2 + I| \neq 0$,
(4) $|B^3 + B + I| \neq 0$, and
(5) $|B^6 + B^5 + B^2 + B + I| \neq 0$,

where B is in $\mathrm{GL}(m, \mathbb{F}_2)$, and $|B|$ means the determinate of B.

Theorem 4. For the matrices of Type (3) in Theorem 2 with $X = A + B$, $YA^2 = I$ and $A^2 = B^2 = X^2$. They are MDS matrices if and only if $|A + I| \neq 0$, where A, B, X, Y are in $\mathrm{GL}(m, \mathbb{F}_2)$, and $|A|$ means the determinate of A.

Please refer to [3] for proofs of theorems in this study.

More constructions. We generalize these structures to $\mathrm{GL}(m, \mathbb{F}_2)$ and directly obtain the lightweight MDS with 10 XOR-counts. Here we give the construction of 4×4 MDS matrix over $\mathrm{GL}(8, \mathbb{F}_2)$ whose XOR count is 10. All the characteristic polynomials of B satisfying the conditions in Theorem 3 can be computed. From the characteristic polynomials we can obtain the corresponding matrices.

For example, we select

$$B = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix},$$

where its characteristic polynomial is $x^8 + x^6 + 1$. Then by equation $AB = I$ and $X = B^2$, we obtain A and X. Then, we obtain an MDS matrix of Type (1) or (2) with 10 XOR-counts. Please note that to illustrate more clearly, we use the symbol $\cdot$ in the matrix to replace 0 here.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 11371356).

References

1 Sarkar S, Syed H. Lightweight diffusion layer: importance of toeplitz matrices. IACR Trans Symmetric Cryptol, 2016, 2016: 95–113
2 Li Y Q, Wang M S. On the construction of lightweight circulant involutory MDS matrices. In: Proceedings of International Conference on Fast Software Encryption. Berlin: Springer, 2016. 121–139
3 Bai J, Li T, Sun Y, et al. The lightest 4×4 MDS matrices over $\mathrm{GL}(4, \mathbb{F}_2)$. Cryptology ePrint Archive, Report 2016/686 (2016). http://eprint.iacr.org/2016/686