Construction of Lightweight MDS Matrices over Matrix Polynomial Residue Ring

Lijing Zhou, Licheng Wang, and Yiru Sun

Beijing University of Posts Telecommunications,Bei Jing, China

Abstract. In this article, we investigate the construction of lightweight MDS matrices. The key contribution of present paper is constructing MDS matrices over matrix polynomial residue ring. To the best of our knowledge, it is the first time that MDS matrices is constructed over matrix polynomial residue ring. In our method, we not only construct vast lightest MDS matrices, but also our algorithm is obvious more efficient than previous papers.

Keywords: MDS matrix, XOR count, matrix polynomial residue ring

1 Introduction

In block cipher, the non-linear confusion layer and the linear diffusion layer are two significant components required for the security of the cipher. The linear diffusion layer with bigger branch number can more effectively resist differential and linear cryptanalysis. The diffusion layer is often constructed by a matrix. For any $n \times n$ matrix, the maximum branch number is $n+1$. Maximum distance separable (MDS) matrix has the maximum branch number.

Many papers choose elements of MDS matrices over finite field [1–6]. The reason is that the size of finite filed is small, and the multiplication and the addition in finite filed are efficient, and the properties of finite field is suitable to construct MDS matrices, for example, any non-zero matrix of a matrix representation of finite field must be non-singular. Although finite field is suitable to construct MDS matrices, it is not suitable to construct lightest MDS matrices. Recently, [7] research construction of lightweight MDS matrices over $GL(m, F_2)$.

2 Preliminaries

In this section, we introduce basic theories and definitions about lightweight MDS matrices and matrix polynomial residue ring.

2.1 MDS Matrices

$GL(n, S)$ denotes the set of all non-singular $n \times n$ matrices with entries in set S. The bundle weight of x is defined as the number of nonzero entries of x

and is expressed by $\omega_b(x)$. For $M \in GL(n, S)$, The branch number of M is the minimum number of nonzero components in the input vector v and output vector $u = M \cdot v$ as we range over all nonzero $v \in S^n$. I.e., the branch number of $n \times n$ matrix M is B_M=$\min_{v \neq 0}\{\omega_b(v) + \omega_b(Mv)\}$,and $B_M \leq n+1$. A maximum distance separable (MDS) $n \times n$ matrix is a matrix that has the optimal branch number $n + 1$.

Eevry linear diffusion layer is a linear map and can be represented by a matrix as follow

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

where $L_{i,j}$ is an $m \times m$ non-singular matrix over F_2, $1 \leq i, j \leq n$, and denote $M(n, m)$ be the set of all matrices like equation (1). For $X = (x_1, x_2, ..., x_n)^T \in (F_2^m)^n$,

$$L(X) = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} L_{1,i}(x_i) \\ \sum_{i=1}^{n} L_{2,i}(x_i) \\ \vdots \\ \sum_{i=1}^{n} L_{n,i}(x_i) \end{pmatrix}, \tag{2}$$

where $L_{i,j}(x_k) = L_{i,j} \cdot x_k$, for $1 \leq i, j \leq n, 1 \leq k \leq n$.

Theorem 1 *Let $L \in M(n, m)$, then L is MDS if and only if all square submatrices of L are of full rank.*

2.2 XOR Count

Let $a, b \in F_2$, $a + b$ is called a bit XOR operation. Let $A \in GL(m, F_2)$, $x = (x_1, x_2, ..., x_m)^T \in F_2^m$, $\#A$ denotes the number of XOR operations required to evaluate Ax directly. Let $\omega(A)$ is the number of 1 in A. So $\#A = \omega(A) - n$, and $\#A$ is also called by XOR count of A. For L$\in M(n, m)$, we denote $\#L = \sum_{i,j=1}^{n} \#L_{ij}$. For instance, let $x = (a, b, c, d)^T \in F_2^4$, and the XOR count of following 4×4 matrix is 4.

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}. \tag{3}$$

$$Ax = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} d \\ c + d \\ b + c + d \\ a + c \end{pmatrix}. \tag{4}$$

3 Our Method and Results

In previous papers, lightweight MDS matrices are constructed over $GF(2^k)$ or $GL(m, F_2)$. In present paper, we construct lightest MDS matrices over matrix polynomial residue ring. In our method, we not only construct vast lightest MDS matrices, but also our algorithm is obvious more efficient than previous papers.

Let A is an $n \times n$ matrix over F_2, and $f(x)$ is the minimum polynomial of A. Because $f(x)$ satisfies $f(A) = 0$, so $F_2[A] \cong F_2[x]/f(x)$. $F_2[A]$ denotes matrix polynomial residue ring generated by A.

Our platform is Intel i5-5300, 2.30GHz with 4GB memory, running Windows 10. We do experiments on follow matrix structures

$$Circulant(I, I, A, B) = \begin{pmatrix} I & I & A & B \\ B & I & I & A \\ A & B & I & I \\ I & A & B & I \end{pmatrix}, Optimal = \begin{pmatrix} A & I & I & I \\ I & I & B & A \\ I & A & I & B \\ I & B & A & I \end{pmatrix},$$

$$Structure\ 1 \begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ I & F & G & I \end{pmatrix}, Structure\ 2 \begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ F & G & I & H \end{pmatrix}.$$

Table 1: **Lightweight MDS Matrices over** 4×4 **Matrix Polynomial Residue Ring**

Matrix type	Sum of XORs	Number	Time
Circulant(I, I, A, B)	12	96	00:00:01
Optimal	13	48	00:00:01
Structure 1	10	288	00:01:40
Structure 2	10	48	00:05:05

Table 2: **Lightweight MDS Matrices over** 8×8 **Matrix Polynomial Residue Ring**

Matrix type	Sum of XORs	Number	Time
Circulant(I, I, A, B)	12	80640	00:01:27
Optimal	10	40320	00:01:16
Structure 1	10	1128960	14:00:00
Hadamard(I,A,B,C)	20	241920	00:07:00
Involutory Hadamard(I,A,B,C)	32	40320	00:03:22

References

1. Sim S M, Khoo K, Oggier F, et al. Lightweight MDS involution matrices[C] //International Workshop on Fast Software Encryption. Springer Berlin Heidelberg, 2015: 471-493.
2. Berger T P, El Amrani N. Codes over mathcal L(GF (2)^m, GF (2)^m), MDS Diffusion Matrices and Cryptographic Applications[C]//International Conference on Codes, Cryptology, and Information Security. Springer International Publishing, 2015: 197-214.
3. Gupta K C, Ray I G. On constructions of MDS matrices from companion matrices for lightweight cryptography[C]//International Conference on Availability, Reliability, and Security. Springer Berlin Heidelberg, 2013: 29-43.
4. Liu M, Sim S M. Lightweight MDS generalized circulant matrices[C]//Fast Software Encryption. 2016.
5. Gupta K C, Ray I G. On constructions of MDS matrices from companion matrices for lightweight cryptography[C]//International Conference on Availability, Reliability, and Security. Springer Berlin Heidelberg, 2013: 29-43.
6. Beierle C, Kranz T, Leander G. Lightweight Multiplication in GF (2^n) with Applications to MDS Matrices[J].
7. Li Y, Wang M. On the construction of lightweight circulant involutory MDS matrices[C]//Fast Software Encryption. 2016.