©2017 Published in 5th International Symposium on Innovative Technologies in Engineering and Science 29-30 September 2017 (ISITES2017 Baku - Azerbaijan)

On Construction of 7×7 Involutory Circulant Matrices

*[1]Mehmet Ozen and [2]Samet Aydogdu
*[1] Faculty of Art and Science, Department of Mathematics Sakarya University, Turkey
[2]Faculty of Art and Science, Department of Mathematics Sakarya University, Turkey

Abstract

We will try to construct 7x7 circulant involutory MDS matrices in which all entries are from a set of mxm nonsingular matrices over finite fields with 2 elements , for m=4 using non-commutative inputs. Here is assumed that the linear transformations used to construct these MDS matrices were not pairwise commutative.

Key words: Ciculant Matrices, Involutory Matrices, MDS Matrices

1. Introduction

Block ciphers are one of the most important building blocks built in most ciphers. Modern block ciphers are frequent repetitions of various rounds. Each round consists of a confusion layer and a diffusion layer. From a mathematical point of view, while diffusion layers are formed by linear functions, confusion layers are usually formed by non-linear (S-boxes) functions. Diffusion layers play an important role in block ciphers as well as in other cryptographic primitives such as hash functions. On the one hand, diffusion layers provide resistance to well known attacks on block ciphers such as differential cryptanalysis and linear cryptanalysis. On the other hand, they greatly influence the efficiency of implementations. In addition, linear diffusion layer is an essential for symmetric ciphers because they provide internal dependency for symmetric encryption algorithms. The quality of a diffusion layer is measured by its number of branches. The larger the number of branches of a diffusion layer in encryption, the better the differential will be against attacks and linear attacks. The cost of implementing a linear diffusion layer in lightweight encryption that aims to provide security in a limited source environment is also important and it has been of particular interest to investigate the problem of building a larger branch of lightweight linear diffusion layer with a rapid evolution of lightweight encryption. A linear diffusion layer is a linear transformation over $(\mathbb{F}_2{}^m)^n$, where m is the S-box in bit length and n is the number of S-boxes. Each linear transformation can be represented by a matrix. In this case, a linear diffusion layer on $(\mathbb{F}_2{}^m)^n$ is represented as a matrix of type $n\times n$, whose inputs appear as linear transformations over $\mathbb{F}_2{}^m$. The maximum number of branches of the matrix of

*Corresponding author: Address: Faculty of Art and Science, Department of Mathematics Sakarya University, 54187, Sakarya TURKEY. E-mail address: ince@sakarya.edu.tr, Phone: +902642955992

type $n \times n$ over $(\mathbb{F}_2^m)^n$ is $n+1$. A linear diffusion layer with a maximum number of branches is called an excellent diffusion layer or matrix that can be separated to a maximum distance (MDS).

The choice of MDS matrices plays an important role in minimizing the area required to ensure safety in a certain amount. There are several ways to construct MDS matrices. Some of them have been given MDS matrices in recursive style [5,7,9]. This structure generally reduces the temporary memory and hardware area required for matrix calculations to a large extent. These recursive matrices are good way to gain space, but the cost of increasing the number of cycles to apply the matrix brings a cost. On the other hand, there are two popular approaches for designing large MDS matrices, one of which is the Cauchy matrices used in [1,3] and the other is the Vandermonde matrices used in [2,4,6]. In addition in [8] some MDS matrices have been constructed using suitable companion matrices for lightweight applications.

Another interesting feature for an MDS matrix in same area is the involution of the matrix. In this case, the MDS matrix itself, which is the involution, will be equal to inverse. This will be of great benefit as it will only mean the use of the matrix itself during the encryption and decryption phase. A common way to construct an MDS matrix is to use MDS codes over the finite field. Multiplication with finite field elements is a fundamental process in evaluating a matrix on the finite field. Usually this process is heavy in practice. Thus, in order to increase the efficiency of the implementations, a matrix must be built with a small number of different finite field elements, and the selected finite field elements must have low Hamming weight. Thus, some matrices can be defined with fewer elements, such as in circulant matrices and Hadamard matrices. These circulant matrices are also investigated in a different way in [12]. On this basis, the lightest MDS matrices have been investigated in [13]. The choice of irreducible polynomials, which have recently been used to calculate multiplication by elements on the finite fields, also has a great effect on efficiently. This has been investigated in the design of algorithms in [10] to investigate lightweight MDS matrices with a small number of XOR operations required to evaluate a row of the corresponding matrix. In [11], a new method for describing a kind of MDS diffusion block matrices with all the blocks on a finite field being polynomials of a given primitive block has been proposed and a series of new MDS matrices have been produced from a MDS matrice discovered a new type transformation that retain the MDS property of the diffusion matrices . In addition, the amount of calculation is greatly reduced when an equivalence relation is obtained from such a transformation and the MDS matrices are searched.

In this study, we will try to construct 7×7 circulant involutory MDS matrices in which all entries are from a set of $m \times m$ nonsingular matrices over $\mathbb{F}_2$, for $m = 4$ using non-commutative inputs , based on the method used to construct the 5×5 circulant involutory MDS matrices in [12].

2. Preliminaries

For $X = (x_1, ..., x_n) \in (\mathbb{F}_2^m)^n$;

$$L(X) = (\sum_{i=1}^{n} L_{1,i}(x_i), ..., \sum_{i=1}^{n} L_{1,i}(x_i)) \ , \tag{1.1}$$

where $L_{i,j}(x_k) = L_{i,j}.x_k$, for $1 \le i, j \le n, 1 \le k \le m$. İf $L \circ L(X) = X$ for $\forall X \in (\mathbb{F}_2^{\ m})^n$, where L^2 is the identity matrix of order mn then a linear diffusion L defined as above is defined as involutory.

For $X = (x_1, ..., x_n) \in (\mathbb{F}_2^{\ m})^n$, the number of nonzero entries of X is defined as the bundle weight of X and $w_b(X)$ denote bundle weight of X. Then

$$w_b(X) = \left|\{x_i : x_i \neq 0, 1 \le i \le n\}\right| \tag{1.2}$$

The branch number of L can be exspressed as the following expression

$$\min\{w_b(X) + w_b(L(X)) \,|\, X \in (\mathbb{F}_2^{\ m})^n, X \neq 0\} \ . \tag{1.3}$$

The matrices equal to the upper bound $n+1$ of L (1.3) are defined to be an MDS matrices.

Square submatrices of L of order t is defined by the matrices

$$L(J,K) = (L_{j_1,k_p}, 1 \le l, p \le t) \tag{1.4}$$

where $J = [j_1, ..., j_t]$ and $K = [k_1, ..., k_n]$ are two sequence of length t, and $1 \le j_1 < ... < j_t \le n$, $1 \le k_1 < ... < k_t \le n$. $L(J,K).(x_1, ..., x_t) = 0$ does not have nonzero solutions $\Leftrightarrow L(J,K)$ of (1.4) is of full rank. Then the following Theorem 1 is true, which is given in [15].

Theorem 1[12]**:** Let $L = (L_{i,j})$, $1 \le i, j \le n$, and the entries of L are $m \times m$ matrices over $\mathbb{F}_2$. Then L is an MDS matrix $\Leftrightarrow$ every square submatrices of L which has order t are of full rank for $1 \le t \le n$.

$Circ(A,B,C,D)$: A circulant matrix is a special kind of Toeplitz matrix in which each row vector is rotated relative to the previous row vector such that

$$Circ(A,B,C,D)=\begin{pmatrix} A & B & C & D \\ D & A & B & C \\ C & D & A & B \\ B & C & D & A \end{pmatrix}$$

where $A,B,C,D \in GL(m,\mathbb{F}_2)$.

3. Main Result

Circulant involutory MDS matrices constructed for $n \le 5$ and $m = 4,8$ are given in [12]. The properties required for involution and MDS of the 5x5 circulant matrices for $n = 5$ and $m = 4,8$ are investigated in [12]. The same results obtained in [12] are used here for the involution and MDS properties of the 7×7 circulant matrices for $n = 7$ and $m = 4$.

Consider the general situation $L = Circ(\mathrm{I}, A, B, C, D, E, F)$. Let's examine the matrix to simplify the characterization in this model and see how the matrices of this type become involutory matrix. First of all, it is necessary for the circulant matrix we define

$$L^2 = Circ(\mathrm{I}, A, B, C, D, E, F).Circ(\mathrm{I}, A, B, C, D, E, F) = Circ(\mathrm{I}, 0, 0, 0, 0, 0, 0)$$

as the general case to be an involutory matrix.

From here, matrix multiplication

$$\mathrm{I}^2 + AF + BE + DC + CD + EB + FA = \mathrm{I}$$

$$A + A + BF + CE + D^2 + EC + FB = 0$$

$$B + A^2 + B + CF + DE + ED + FC = 0$$

$$C + AB + BA + C + DF + E^2 + FD = 0$$

$$D + AC + B^2 + CA + D + EF + FE = 0$$

$$E + AD + BC + CB + DA + E + F^2 = 0$$

$$F + AE + BD + C^2 + DB + EA + F = 0 \qquad (1.5)$$

Equations are obtained. To simplify these given equations (1.5), taking $F = A$, $E = B$, $D = C$ and taking into account that we are working over $\mathbb{F}_2$

$$\mathrm{I}^2 = \mathrm{I}$$

$$C^2 + BA + AB + CB + BC = 0$$

$$A^2 + CA + AC + CB + BC = 0$$

$$B^2 + AB + BA + CA + AC = 0 \tag{1.6}$$

Equations are obtained. As you can see from (1.6), it means that

$$L = Circ(\mathrm{I}, A, B, C, D, E, F) = Circ(\mathrm{I}, A, B, C, C, B, A) \tag{1.7}$$

.

Then, let's now look at Lemma 1 given below, where 7×7 $L = Circ(\mathrm{I}, A, B, C, C, B, A)$ circulant matrix is the involutory.

Lemma 1: Let $L = Circ(\mathrm{I}, A, B, C, C, B, A)$ for $A, B, C \in GL(4, \mathbb{F}_2)$ be circulant matrix. Then L is an involution if and only if

$$A^2 = AC + CA + BC + CB,$$

$$B^2 = AB + BA + AC + CA,$$

$$C^2 = AB + BA + BC + CB \tag{1.8}$$

hold simultaneously.

Proof:

$$L^2 = Circ(\mathrm{I}, A, B, C, C, B, A).Circ(\mathrm{I}, A, B, C, C, B, A)$$
$$= Circ(\mathrm{I}^2, BA + CB + C^2 + BC + AB, A^2 + CA + CB + BC + AC, AB + BA + CA + B^2 + AC$$
$$, AB + BA + CA + B^2 + AC, A^2 + CA + AC + CB + BC, BA + AB + CB + BC + C^2) \tag{1.9}$$

Here L is an involution if and only if $L^2 = Circ(\mathrm{I}, 0, 0, 0, 0, 0, 0)$. That is

$$\mathrm{I}^2 = \mathrm{I}$$

$$BA + CB + C^2 + BC + AB = 0$$

$$A^2 + CA + CB + BC + AC = 0$$

$$AB + BA + CA + B^2 + AC = 0$$

$$AB + BA + CA + B^2 + AC = 0$$

$$A^2 + CA + AC + CB + BC = 0$$

$$BA + AB + CB + BC + C^2 = 0 \qquad (1.10)$$

.

Therefore from (1.10), L circulant matrix is an involution. Now let's look at the MDS property of the L circulant matrix. For a matrix to be an MDS matrix, all its square submatrices must be nonsingular. Based on this situation, let us give the following theorem.

Theorem 2 [14]**:** A square matrix M is invertible if and only if the homogeneous system $M.x = 0$ has no non-zero solutions.

Proof: First, suppose that M^{-1} exists. Then $M.x = 0 \Rightarrow x = M^{-1}.0 = 0$.

Thus, if M is invertible, then $M.x = 0$ has no non-zero solutions.

On the other hand, $M.x = 0$ always has the solution $x = 0$ .If no other solutions exist, then M can be put into reduced row echelon form with every variable a pivot. In this case, M^{-1} can be computed.

Let's look at whether the L circulant matrix is MDS with the aid of this theorem and lemma2 given below.

Lemma 2 [12]**:** Suppose $A, B, C \in GL(m, \mathbb{F}_2)$ are $m \times m$ nonsingular matrices over $\mathbb{F}_2$. Then the following statements hold.

1) $\begin{pmatrix} \mathrm{I} & A \\ B & C \end{pmatrix}$ is of full rank $\Leftrightarrow rank(BA + C) = m$.
2) $\begin{pmatrix} A & \mathrm{I} \\ B & C \end{pmatrix}$ is of full rank $\Leftrightarrow rank(CA + B) = m$.
3) $\begin{pmatrix} A & B \\ \mathrm{I} & C \end{pmatrix}$ is of full rank $\Leftrightarrow rank(AC + B) = m$.
4) $\begin{pmatrix} A & B \\ C & \mathrm{I} \end{pmatrix}$ is of full rank $\Leftrightarrow rank(BC + A) = m$.

Let us first investigate whether the 2×2 submatrices of the 7×7 $L = Circ(\mathrm{I}, A, B, C, C, B, A)$ circulant matrices for $m = 4$ are nonsingular. The $L = Circ(\mathrm{I}, A, B, C, C, B, A)$ circulant matrice has 441 units 2×2 submatrices for any $A, B, C \in GL(4, \mathbb{F}_2)$ matrices.

For $A,B,C \in GL(4,\mathbb{F}_2)$ and $X=(x_1,...,x_7) \in (\mathbb{F}_2{}^4)^7$ the cases where the 2×2 submatrices of the circulant matrix L are nonsingular, are checked with the help of the above lemma 2. Here the following indefinite states are obtained from the checked states.

$(A+B).x_1+(B+C).x_5=0$ $(A+C).x_1+(B+C).x_2=0$ $(A+B).x_1+(A+C).x_3=0$
$(A+B).x_1+(B+C).x_7=0$ $(A+C).x_1+(B+C).x_3=0$ $(A+B).x_1+(A+C).x_4=0$
$(A+B).x_1+(B+C).x_2=0$ $(A+C).x_1+(B+C).x_6=0$ $(A+B).x_1+(A+C).x_5=0$
$(A+B).x_1+(B+C).x_4=0$ $(A+C).x_1+(B+C).x_7=0$ $(A+B).x_1+(A+C).x_6=0$
$(A+B).x_2+(B+C).x_3=0$ $(A+C).x_2+(B+C).x_1=0$ $(A+B).x_2+(A+C).x_4=0$
$(A+B).x_2+(B+C).x_5=0$ $(A+C).x_2+(B+C).x_3=0$ $(A+B).x_2+(A+C).x_5=0$
$(A+B).x_2+(B+C).x_6=0$ $(A+C).x_2+(B+C).x_4=0$ $(A+B).x_2+(A+C).x_6=0$
$(A+B).x_2+(B+C).x_1=0$ $(A+C).x_2+(B+C).x_7=0$ $(A+B).x_2+(A+C).x_7=0$
$(A+B).x_3+(B+C).x_4=0$ $(A+C).x_3+(B+C).x_4=0$ $(A+B).x_3+(A+C).x_1=0$
$(A+B).x_3+(B+C).x_6=0$ $(A+C).x_3+(B+C).x_5=0$ $(A+B).x_3+(A+C).x_5=0$
$(A+B).x_3+(B+C).x_2=0$ $(A+C).x_3+(B+C).x_1=0$ $(A+B).x_3+(A+C).x_6=0$
$(A+B).x_3+(B+C).x_7=0$ $(A+C).x_3+(B+C).x_2=0$ $(A+B).x_3+(A+C).x_7=0$
$(A+B).x_4+(B+C).x_5=0$ $(A+C).x_4+(B+C).x_2=0$ $(A+B).x_4+(A+C).x_1=0$
$(A+B).x_4+(B+C).x_7=0$ $(A+C).x_4+(B+C).x_3=0$ $(A+B).x_4+(A+C).x_2=0$
$(A+B).x_4+(B+C).x_1=0$ $(A+C).x_4+(B+C).x_5=0$ $(A+B).x_4+(A+C).x_6=0$
$(A+B).x_4+(B+C).x_3=0$ $(A+C).x_4+(B+C).x_6=0$ $(A+B).x_4+(A+C).x_7=0$
$(A+B).x_5+(B+C).x_1=0$ $(A+C).x_5+(B+C).x_3=0$ $(A+B).x_5+(A+C).x_1=0$
$(A+B).x_5+(B+C).x_6=0$ $(A+C).x_5+(B+C).x_4=0$ $(A+B).x_5+(A+C).x_2=0$
$(A+B).x_5+(B+C).x_2=0$ $(A+C).x_5+(B+C).x_6=0$ $(A+B).x_5+(A+C).x_3=0$
$(A+B).x_5+(B+C).x_4=0$ $(A+C).x_5+(B+C).x_7=0$ $(A+B).x_5+(A+C).x_7=0$
$(A+B).x_6+(B+C).x_3=0$ $(A+C).x_6+(B+C).x_1=0$ $(A+B).x_6+(A+C).x_1=0$
$(A+B).x_6+(B+C).x_2=0$ $(A+C).x_6+(B+C).x_4=0$ $(A+B).x_6+(A+C).x_2=0$
$(A+B).x_6+(B+C).x_7=0$ $(A+C).x_6+(B+C).x_5=0$ $(A+B).x_6+(A+C).x_3=0$
$(A+B).x_6+(B+C).x_5=0$ $(A+C).x_6+(B+C).x_7=0$ $(A+B).x_6+(A+C).x_4=0$
$(A+B).x_7+(B+C).x_4=0$ $(A+C).x_7+(B+C).x_1=0$ $(A+B).x_7+(A+C).x_2=0$
$(A+B).x_7+(B+C).x_6=0$ $(A+C).x_7+(B+C).x_2=0$ $(A+B).x_7+(A+C).x_3=0$
$(A+B).x_7+(B+C).x_1=0$ $(A+C).x_7+(B+C).x_5=0$ $(A+B).x_7+(A+C).x_4=0$
$(A+B).x_7+(B+C).x_3=0$ $(A+C).x_7+(B+C).x_6=0$ $(A+B).x_7+(A+C).x_5=0$

For a matrix to be an MDS matrix, all square submatrices must be nonsingular, and if any of these square submatrices does not provide this condition, then the matrix is not a MDS matrix. As in the above theorem, A square matrix A is nonsingular if and only if the homogeneous system $A.x = 0$ has no non-zero solutions so that the homogeneous system $A.x = 0$ only has a solution of $x = 0$. However, since the situation given in theorem 2 can not be discussed in the above cases, the matrices $(A+B)$, $(A+C),(B+C)$ obtained from matrices $A,B,C \in GL(4,\mathbb{F}_2)$ can not be nonsingular. Therefore, it is not necessary to check whether $3\times3, 4\times4$, $5\times5, 6\times6$, 7×7 square submatrices are nonsingular matrices since all 2×2 submatrices are not nonsingular. If all square submatrices of 2×2 were nonsingular, the Theorem 1 would be used to check whether all the other square submatrices are nonsingular matrices.

As a result, then the $L = Circ(\mathrm{I}, A, B, C, C, B, A)$ involutory circulant matrix is not the MDS matrix.

4. Conclusion

In the study, we have tried to construct 7×7 circulant involution MDS matrices in which all entries are from a set of $m\times m$ nonsingular matrices over $\mathbb{F}_2$, for $m = 4$ using non-commutative inputs. We were able to provide the involutory feature but we could not provide the MDS because of the obstacles given in the study.

References

1. Youssef, A.M., Mister, S., Tavares, S.E.: On the Design of Linear Transformations for Substitution Permutation Encryption Networks. SAC'97, pp. 1-9, 1997.
2. Lacan, J., Fimes, J.: Systematic MDS Erasure Codes Based on Vandermonde Matrices. IEEE Trans. Commun. Lett., vol 8(9), pp. 570-572, 2004.
3. Nakara Jr, J., Abrahao, E.: A New Involutory MDS Matrix for the AES. International Journal of Network Security, vol. 9(2), pp. 109-116, 2009.
4. Sajadieh, M., Dakhilalian, M., Mala, H., Omoomi, B.: On Construction of Involutory MDS Matrices from Vandermonde Matrices in $GF(2^q)$. Des. Codes Cryptogr., vol. 64, pp. 287-308, Springer, 2012.
5. Sajadieh, M., Dakhilalian, M., Mala, H., Sepehrdad, P.: Recursive Diffusion Layers for Block Ciphers and Hash Functions. FSE 2012, LNCS, vol. 7549, pp. 385-401, Springer, 2012.
6. Gupta, K.C., Ray, I.G.: On Constructions of Involutory MDS Matrices. In AFRICACRYPT 2013, pp. 43-60, Springer, 2013.
7. Augot, D., Finiasz, M.: Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions. In ISIT, pp. 1551-1555, 2013.

8. Gupta, K.C., Ray, I.G.: On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography. CD-ARES 2013 Workshops, LNCS, vol. 8128, pp. 29-43, Springer, 2013.
9. Berger, T.P.: Construction of Recursive MDS Diffusion Layers from Gabidulin Codes. INDOCRYPT 2013, LNCS, vol. 8250, pp. 274-285, Springer, 2013.
10. Sim, S.M., Khoo, K., Oggier, F., Peyrin, T.: Lightweight MDS Involution Matrices. In: Leander, G., Demirci, H. (eds.) FSE 2015, LNCS, Springer, 2015.
11. Zhao, R., Zhang, R., Li, Y., Wu, B.: On Constructions of a Sort of MDS Block Diffusion Matrices for Block Ciphers and Hash Functions. IACR Cryptology ePrint Archive . 2015.
12. Li, Y., Wang, M.: On the Constructions of Lightweight Circulant Involutory MDS Matrices. In: FSE. LNCS, Springer, 2016.
13. Bai, J., Wang, D.: The Lightest 4×4 MDS Matrices over $GL(4,\mathbb{F}_2)$. Cryptology ePrint Archive: Report 2016/1131, 2016.
14. Cherney, D., Denton, T., Thomas, R., Waldron, A.: Linear Algebra. pp. 154, Davis California, 2013.
15. Blaum, M., Roth, R.M.: On Lowest Density MDS Codes. IEEE Transactions on Information Theory 45(1), pp. 46-59, 1999.