Efficient MDS Diffusion Layers Through Decomposition of Matrices

S. M. Dehnavi  
Kharazmi University  
Faculty of Mathematical and Computer Sciences  
Tehran, Iran  
std_dehnavism@khu.ac.ir

M. R. Mirzaee Shamsabad  
Shahid Bahonar University  
Faculty of Mathematics and Computer Science  
Kerman, Iran  
mohammadmirzaeesh@yahoo.com

A. Mahmoodi Rishakani  
Shahid Rajaee Teacher Training University  
Faculty of Sciences  
Tehran, Iran  
am.rishakani@srttu.edu

Y. Fekri Dabanloo  
Shahid Rajaee Teacher Training University  
Faculty of Sciences  
Tehran, Iran  
yousef.fekri@srttu.edu

Abstract — Diffusion layers are critical components of symmetric ciphers. MDS matrices are diffusion layers of maximal branch number which have been used in various symmetric ciphers. In this article, we examine decomposition of cyclic matrices from mathematical viewpoint and based on that, we present new cyclic MDS matrices. From the aspect of implementation, the proposed matrices have lower implementations costs both in software and hardware, compared to what is presented up to now. In Section 2, we present preliminary notations and definitions. Section 3 is devoted to MDS matrices with efficient implementation and Section 4 is the conclusion.

Keywords — Diffusion layer; MDS matrix; Symmetric cipher; Decomposition of matrices;

I. INTRODUCTION

Diffusion layers are crucial components of symmetric ciphers. MDS matrices are diffusion layers with maximum branch number. MDS diffusion layers are used in several symmetric ciphers [1-7]. Some aspects of the theory of MDS diffusion layers is studied in [8-14].

In this article, we verify a special kind of MDS matrices, namely cyclic MDS matrices and propose new MDS matrices of this type. The presented matrices have lower implementation costs compared to what is presented up to now. In [10,15,16] diffusion layers in the form of a matrix power are examined. In this paper, we study decomposition of matrices from another viewpoint: we consider the product of matrices and then check these products for MDSness.

More precisely, we study cyclic matrices over finite fields of characteristic 2 and based upon this algebraic investigation, we provide some $4 \times 4$ and $8 \times 8$ MDS matrices with efficient implementation.

II. PRELIMINARY NOTATIONS AND DEFINITIONS

Let $R$ be a finite commutative ring with identity. We denote the ring of polynomials over $R$ by $R[x]$. Suppose that $p(x) \in R[x]$; the ring of polynomials modulo $p(x)$ is denoted by $\frac{R[x]}{<p(x)>}$.

Throughout the paper, $m, n, r$ and $t$ are natural numbers. The finite field of order $2^n$ is denoted by $F_{2^n}$ and the Cartesian product of $n$ copies of $F_2$ by $F_{2^n}^n$. Cardinality of a finite set $A$ is denoted by $|A|$. We denote the operation of addition in $F_{2^n}$ by $\oplus$. Addition in $F_{2^n}[x]$ and the XOR operation in $F_{2^n}^t$ is denoted by $\oplus$. We denote left rotation by $\ll$ and composition of functions by $\circ$. The zero vector of any size is denoted by $\mathbf{0}$. We use the notation $\equiv$ for equivalence of sets, functions, vectors or algebraic structures.

Let $F_{2^m}^m$ be the natural $m$-dimensional linear space over $F_{2^n}$. Let $x = (x_{m-1}, \ldots, x_0) \in F_{2^m}^m$ be a vector of length $m$. The weight of $x$ is denoted by $w(x)$ and is defined as $w(x) = |\{0 \leq i < m: x_i \neq 0\}|$.

The (differential) branch number of a linear transformation $\psi: F_{2^m}^m \rightarrow F_{2^m}^m$ or its representing matrix is defined as $\min_{x \in F_{2^m}^m-\{0\}} \{w(x) + w(\psi(x))\}$.

A linear transformation $\psi: F_{2^m}^m \rightarrow F_{2^m}^m$ is called MDS [17,18] iff its branch number is equal to $m + 1$. 

III. CONSTRUCTION OF NEW MDS MATRICES

At first, we prove a theorem which is the base for applications presented in this paper.

**Theorem 1.** Let $R = \frac{F_{2^n}[x]}{x^r+1}$. Every $p \in R$ of the form

$$r - 1 \bigoplus p_i x^i$$

corresponds to a mapping

$$\psi_p: R \rightarrow R,$$

$$\psi_p(a) = pa \ mod \ (x^r \oplus 1).$$

Further, there is an $r \times r$ matrix $P$ over $F_{2^n}$ which is the representing matrix of a linear transformation $\psi_p$ such that the action of $\psi_p$ and $\psi_p$ are exactly the same:

$$\psi_p: F_{2^n}^r \rightarrow F_{2^n}^r,$$

$$a \equiv (a_{r-1}, \ldots, a_0) \mapsto (a_{r-1}, \ldots, a_0)P \equiv pa \ mod \ (x^r \oplus 1).$$

Here,

$$P = [p_{ij}]_{r \times r}, \quad p_{ij} = p_{(i-j) \ mod \ r}.$$

**Proof.** We know that $a$ is of the form

$$r - 1 \bigoplus a_i x^i$$

and so, if we take

$$r - 1 \bigoplus q_i x^i = pa \ mod \ (x^r \oplus 1),$$

then we have

$$q_i = \sum_{j=0}^{r-1} p_j a_{(i-j) \ mod \ r}, \quad 0 \leq i < r.$$

Here, the symbol $\sum$ stands for addition in $F_{2^n}$. Now, if we consider the action of the linear transformation $\psi_p$, we have

$$(a_{r-1}, \ldots, a_0) \mapsto (a_{r-1}, \ldots, a_0)P,$$

with

$$P = [p_{ij}]_{r \times r}, \quad p_{ij} = p_{(i-j) \ mod \ r}.$$

**Note 2.** The correspondence investigated in Theorem 1 is such that for $p, p_1, p_2 \in R$ with $p = p_1 p_2$, we have $P = P_1 P_2$. Here, $P_1$ is the corresponding matrix of $p_1$ and $P_2$ is the corresponding matrix of $p_2$. Moreover, for an invertible element $p \in \frac{F_{2^n}[x]}{x^r+1}$, $p^{-1}$ corresponds to $P^{-1}$.

Now, we recall the mapping given in [19, Exam. 6] as an example of Theorem 1. We note that Theorem 1 is somewhat a generalization of the concepts presented in [19].

**Example 3.** Consider the mappings

$$f_1, f_2, f_3: F_{2^2}^r \rightarrow F_{2^2}^r,$$

$$f_1(x) = x \oplus (x \ll 1) \oplus (x \ll 2),$$

$$f_2(x) = x \oplus (x \ll 2) \oplus (x \ll 7),$$

$$f_3(x) = x \oplus (x \ll 4) \oplus (x \ll 10),$$

and $f(x) = f_1 \circ f_2 \circ f_3(x)$. Then, $f$ has branch number 12 over $F_{2^n}$ for any $n$.

In Example 3, we have used the concept of decomposition of matrices over $F_2$ or factoring of polynomials in $\frac{F_2[x]}{x^{2^2}+1}$ to find a linear mapping of maximal branch number with more efficient implementation, compared to what is presented up to now.

Now we have an example in finite field $F_{2^n}$, $n > 1$.

**Example 4.** Consider $R = \frac{F_{2^n}[x]}{x^3+1}$. Let $p, a \in R$ with

$$p = p_0 \oplus p_1 x \oplus p_2 x^2,$$

$$a = a_0 \oplus a_1 x \oplus a_2 x^2.$$

We have

$$pa \ mod \ (x^3 \oplus 1) = (p_0 a_0 + p_2 a_1 + p_1 a_2)$$

$$\oplus (p_0 a_1 + p_1 a_0 + p_2 a_2)x$$

$$\oplus (p_0 a_2 + p_1 a_1 + p_2 a_0)x^2.$$

With matrix notations, we have

$$pa \ mod \ (x^3 \oplus 1) \equiv (a_2 \ a_1 \ a_0) \begin{pmatrix} p_0 & p_2 & p_1 \\ p_1 & p_0 & p_2 \\ p_2 & p_1 & p_0 \end{pmatrix}.$$

So, the corresponding matrix of $p$ would be

$$P = \begin{pmatrix} p_0 & p_2 & p_1 \\ p_1 & p_0 & p_2 \\ p_2 & p_1 & p_0 \end{pmatrix}.$$

**Construction 5.** Let $\alpha \in F_{2^n}$. Consider $R = \frac{F_{2^n}[x]}{x^3+1}$ and $p, p_1, p_2 \in R$ with $p = p_1 p_2 \ mod \ (x^3 \oplus 1)$, and

$$p_1 = x^3 \oplus \alpha,$$

$$p_2 = x^3 \oplus x \oplus 1.$$

We have

$$p = (\alpha + 1)x^3 \oplus x^2 \oplus \alpha x \oplus (\alpha + 1).$$

The corresponding matrices are

$$P_1 = \begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 1 & 0 \\ 0 & 0 & \alpha & 1 \\ 1 & 0 & 0 & \alpha \end{pmatrix}.$$
\[ P_2 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \]
and
\[ P = \begin{pmatrix} \alpha + 1 & \alpha + 1 & 1 & \alpha \\ \alpha & \alpha + 1 & \alpha + 1 & 1 \\ 1 & \alpha & \alpha + 1 & \alpha + 1 \\ \alpha + 1 & 1 & \alpha & \alpha + 1 \end{pmatrix}. \]

It can be verified that the conditions on \( \alpha \) to make \( P \) MDS over \( F_{2^n} \), is the same as conditions of \([12, Coro. 4.5]: \alpha, \alpha^3 + 1 \) and \( \alpha^3 + 1 \) should not be zero. So, as stated after that corollary, almost all elements \( \alpha \) in \( F_{2^n} \), make \( P \) MDS.

If we wish to use the diffusion layer corresponding to \( P \), the pseudo-code for implementing it, would be as follows:

\[ Z_3 = \alpha X_3 \oplus X_0, \]
\[ Z_2 = \alpha X_2 \oplus X_3, \]
\[ Z_1 = \alpha X_1 \oplus X_2, \]
\[ Z_0 = \alpha X_0 \oplus X_1, \]
\[ T_1 = Z_3 \oplus Z_2, \]
\[ T_2 = Z_1 \oplus Z_0, \]
\[ Y_3 = T_1 \oplus Z_0, \]
\[ Y_2 = T_1 \oplus Z_1, \]
\[ Y_1 = T_2 \oplus Z_2, \]
\[ Y_0 = T_2 \oplus Z_3. \]

Here, \( X_i \)'s, \( 0 \leq i \leq 3 \), are the inputs, \( Y_i \)'s, \( 0 \leq i \leq 3 \), are the outputs and \( Z_i \)'s, \( 0 \leq i \leq 3 \), and \( T_i \)'s, \( 1 \leq i \leq 2 \), are temporary variables.

**Note 6.** If we replace \( F_{2^n} \) in Construction 5 with any finite commutative ring with identity \( S \), or \( F_{2^n[x]} / \langle x^4 + 1 \rangle \) with \( F_{2^n[x]} / \langle x^8 + 1 \rangle \), then the conditions for MDSness of \( P \) are invertibility of \( \alpha, \alpha^3 + 1 \) and \( \alpha^7 + 1 \) in the ring \( S \). These conditions are the same as conditions of \([10, Theo. 7] \) and so, every matrix \( L \) (instead of \( \alpha \)) satisfying the conditions of that theorem, satisfies the conditions for MDSness of \( P \). The important point concerning the decomposition done in Construction 5 is that, the cost of implementing this decomposition is 10 XOR’s and 4 table lookups or field multiplications. Compared to the best matrices given in \([10] \) which need 14 XOR’s and 4 table lookups or field multiplications, our proposed matrix saves 4 XOR operations.

One of the drawbacks of our method is that the cost of implementing the inverse of these cyclic matrices is high and there are no involutions of this type. For example, for Construction 5 we have

\[ (x^3 \oplus \alpha)^{-1} = \alpha^2 (\alpha + 1)^{-1} x \oplus \alpha (\alpha + 1)^{-1} x^2. \]
with
\[ P = \left[ p_{ij} \right]_{a \times a'} \]
\[
p_{ij} = \begin{cases} 
ab & (i - j) \mod 8 = 0 \\
abc + 1 & (i - j) \mod 8 = 1 \\
a & (i - j) \mod 8 = 2 \\
ac + b & (i - j) \mod 8 = 3 \\
ab + bc & (i - j) \mod 8 = 4 \\
1 & (i - j) \mod 8 = 5 \\
a + c & (i - j) \mod 8 = 6 \\
b & (i - j) \mod 8 = 7 \\
\end{cases}, \quad 0 \leq i, j < 8.
\]

We have searched these matrices for MDSness by symbolic computation programming. The following parameters in any field \( F_{2^n} \) with \( n \geq 8 \) satisfy the conditions for MDSness of \( P \):
\[
a = \alpha + 1, \\
b = \alpha^2 + \alpha + 1, \\
c = \alpha^3 + \alpha + 1,
\]
where \( \alpha \) is a primitive element in \( F_{2^n} \). In fact, we have used symbolic computations and found all of the determinants: there were 930 distinct polynomials. The subtle point here is that the degree of all these polynomials (symbolic determinants) is less than 255. So, any \( \alpha \) which is not a root of these polynomials, satisfy the conditions for MDSness of \( P \).

From the practical aspect, we can use any primitive element of \( F_{2^n} \), are the outputs and \( Y_i \)'s, and cannot be a root of any polynomial over \( F_{2^n} \) with degree less than \( 2^n - 1 \geq 255 \). Of course, we can use a primitive polynomial as the defining polynomial of \( F_{2^n} \). In this case, \( \alpha = x \) would be a primitive element which is the best case from implementation viewpoint. By checking different primitive polynomials as defining polynomial of \( F_{2^n} \), we can find the best primitive polynomial which yields the best implementation in hardware.

As in Construction 5, if \( X_i \)'s, \( 0 \leq i \leq 7 \), are the inputs, \( Y_i \)'s, \( 0 \leq i \leq 7 \), are the outputs and \( Z_i \)'s and \( T_i \)'s, \( 0 \leq i \leq 7 \), are temporary variables, then we have
\[
Z_7 = aX_0 \oplus X_3, \\
Z_6 = aX_7 \oplus X_2, \\
Z_5 = aX_6 \oplus X_4, \\
Z_4 = aX_5 \oplus X_0, \\
Z_3 = aX_4 \oplus X_7, \\
Z_2 = aX_3 \oplus X_6, \\
Z_1 = aX_2 \oplus X_5, \\
Z_0 = aX_1 \oplus X_4.
\]
\[
T_7 = bZ_0 \oplus Z_2, \\
T_6 = bZ_7 \oplus Z_1, \\
T_5 = bZ_6 \oplus Z_0, \\
T_4 = bZ_5 \oplus Z_7, \\
T_3 = bZ_4 \oplus Z_6, \\
T_2 = bZ_3 \oplus Z_5, \\
T_1 = bZ_2 \oplus Z_4, \\
T_0 = bZ_1 \oplus Z_3.
\]

The implementation of \( P \), needs 32 XOR’s and 24 table lookups or field multiplications, which has lower implementation cost in comparison to what is presented in [8] for \( 8 \times 8 \) MDS matrices; the best implementation of [8] needs 43 table lookups plus 56 XOR’s. Of course, our proposed matrix can be compared with the \( 8 \times 8 \) MDS matrices of [10]. The best implementation of [10, Tab. 4] needs 16 table lookups plus 80 XOR’s, which has higher implementation cost than our proposed matrix in typical processors.

IV. CONCLUSION

Diffusion layers are important components of symmetric ciphers. MDS matrices have been used in several symmetric ciphers. In this article, we studied decomposition of cyclic matrices from mathematical viewpoint and based on that, we presented new cyclic MDS matrices.

From the aspect of implementation, the proposed matrices have lower implementations costs both in software and hardware, compared to what is presented in cryptographic literature, up to our knowledge.

We think that based on the theory presented in this paper, the search for optimum MDS matrices over finite fields or finite commutative rings with identity can be done and more efficient matrices can be found by this method.
REFERENCES


