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 in cryptographic literature, up to our knowledge.**

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 two and based upon this algebraic investigation, we provide some 4×4 MDS matrices with efficient implementation.

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.

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. Cardinality of a finite set A is denoted by $|A|$. We denote the operation of addition in F_{2^n} by $+$. Addition in $F_{2^n}[x]$ and the XOR operation in F_2^n is denoted by $\oplus$. We denote left rotation by $\lll$ 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 $F_{2^n}^m$ be the natural m-dimensional linear space over F_{2^n}. Let $x = (x_{m-1}, \dots, x_0) \in F_{2^n}^m$ 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 $\psi: F_{2^n}^m \to F_{2^n}^m$ or its representing matrix is defined as

$$min_{x \in F_{2^n}^m - \{\mathbf{0}\}} \{w(x) + w(\psi(x))\}.$$

A linear transformation $\psi: F_{2^n}^m \to F_{2^n}^m$ 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 $R = \frac{F_{2^n}[x]}{<x^r \oplus 1>}$. Every $p \in R$ of the form

$$\bigoplus_{i=0}^{r-1} p_i x^i$$

corresponds to a mapping

$$\psi_p: R \to R,$$
$$\psi_p(a) = pa \ mod \ (x^r \oplus 1).$$

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

$$\psi_P: F_{2^n}^r \to F_{2^n}^r,$$
$$a \equiv (a_{r-1}, \dots, a_0) \longmapsto (a_{r-1}, \dots, a_0)P \equiv pa \ mod \ (x^r \oplus 1).$$

Here,

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

Proof. We know that a is of the form

$$\bigoplus_{i=0}^{r-1} a_i x^i$$

and so, if we take

$$\bigoplus_{i=0}^{r-1} q_i x^i = pa \ mod \ (x^r \oplus 1),$$

then we have

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

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

$$(a_{r-1}, \dots, a_0) \longmapsto (a_{r-1}, \dots, a_0)P,$$

with

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

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 $p \in \frac{F_{2^n}[x]}{<x^r \oplus 1>}$, 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

$$f_1, f_2, f_3, f: F_2^{32} \to F_2^{32},$$
$$f_1(x) = x \oplus (x \lll 1) \oplus (x \lll 2),$$
$$f_2(x) = x \oplus (x \lll 2) \oplus (x \lll 7),$$
$$f_3(x) = x \oplus (x \lll 4) \oplus (x \lll 10),$$

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 $\frac{F_2[x]}{<x^{32} \oplus 1>}$, 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 $R = \frac{F_{2^n}[x]}{<x^3 \oplus 1>}$. 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

$$\begin{aligned} pa \ mod \ (x^3 \oplus 1) = & (p_0 a_0 + p_2 a_1 + p_1 a_2) \\ & \oplus (p_0 a_1 + p_1 a_0 + p_2 a_2)x \\ & \oplus (p_0 a_2 + p_1 a_1 + p_2 a_0)x^2. \end{aligned}$$

With matrix notations, we have

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

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 $R = \frac{F_{2^n}[x]}{<x^4 \oplus 1>}$ and $p, p_1, p_2 \in R$ with $p = p_1 p_2 \ mod \ (x^4 \oplus 1)$, 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 α to make P MDS over F_{2^n}, is the same as conditions of [12, Coro. 4.5]: α, α^3+1 and α^7+1 should not be zero. So, as stated after that corollary, almost all elements α 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, $0 \le i \le 3$, are the inputs, Y_i's, $0 \le i \le 3$, are the outputs and Z_i's, $0 \le i \le 3$, and T_i's, $1 \le i \le 2$, are temporary variables.

Note 6. If we replace F_{2^n} in Construction 5 with any finite commutative ring with identity S, or $\frac{F_{2^n}[x]}{<x^4 \oplus 1>}$ with $\frac{S[x]}{<x^4 \oplus 1>}$, then the conditions for MDSness of P are invertibility of α, α^3+1 and α^7+1 in the ring S. These conditions are the same as conditions of [10, Theo. 7] and so, every matrix L (instead of α) 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

$$(x^3 \oplus \alpha)^{-1} = \alpha^2(\alpha+1)^{-4}x^3 \oplus \alpha(\alpha+1)^{-4}x^2$$
$$\oplus (\alpha+1)^{-1}x \oplus \alpha^3(\alpha+1)^{-4},$$

$$(x^3 \oplus x \oplus 1)^{-1} = x^3 \oplus x \oplus 1,$$

and

$$\left((\alpha+1)x^3 \oplus x^2 \oplus \alpha x \oplus (\alpha+1)\right)^{-1}$$
$$= (\alpha^3+\alpha^2+\alpha)(\alpha+1)^{-4}x^3$$
$$\oplus (\alpha^2+\alpha+1)(\alpha+1)^{-4}x^2$$
$$\oplus (\alpha^3+\alpha+1)(\alpha+1)^{-4}x$$
$$\oplus (\alpha^3+\alpha^2+1)(\alpha+1)^{-4}.$$

Of course, if we apply the matrix of Construction 5 in a Feistel scheme or in an SPN structure in a mode like CTR, which do not need the implementation of the inverse of mappings, then our method is more efficient.

Construction 6. Let $R = \frac{F_{2^n}[x]}{<x^8 \oplus 1>}$. We take

$$p = (x^3 \oplus a)(x^2 \oplus b)(x^4 \oplus cx \oplus 1) \ mod \ (x^8 \oplus 1)$$
$$= bx^7 \oplus (a+c)x^6 \oplus x^5 \oplus (ab+bc)x^4$$
$$(ac+b)x^3 \oplus ax^2 \oplus (abc+1)x + ab.$$

Here, $p = p_1 p_2 p_3 \ mod \ (x^8 \oplus 1)$ with

$$p_1 = x^3 \oplus a,$$
$$p_2 = x^2 \oplus b,$$
$$p_3 = x^4 \oplus cx \oplus 1.$$

The corresponding matrices are

$$P_1 = \left[p^1_{ij}\right]_{8\times 8},$$

with

$$p^1_{ij} = \begin{cases} a & (i-j) \ mod \ 8 = 0 \\ 1 & (i-j) \ mod \ 8 = 3 \\ 0 & (i-j) \ mod \ 8 \ne 0,3 \end{cases}, \quad 0 \le i < 8, \ \ 0 \le j < 8.$$

$$P_2 = \left[p^2_{ij}\right]_{8\times 8},$$

with

$$p^2_{ij} = \begin{cases} b & (i-j) \ mod \ 8 = 0 \\ 1 & (i-j) \ mod \ 8 = 2 \\ 0 & (i-j) \ mod \ 8 \ne 0,2 \end{cases}, \quad 0 \le i < 8, \ \ 0 \le j < 8.$$

$$P_3 = \left[p^3_{ij}\right]_{8\times 8},$$

with

$$p^3_{ij} = \begin{cases} 1 & (i-j) \ mod \ 8 = 0,4 \\ c & (i-j) \ mod \ 8 = 1 \\ 0 & (i-j) \ mod \ 8 \ne 0,1,4 \end{cases}, \quad 0 \le i < 8, \ \ 0 \le j < 8,$$

and

$$P = [p_{ij}]_{8\times 8},$$

with

$$p_{ij} = \begin{cases} ab & (i-j)\ mod\ 8 = 0 \\ abc+1 & (i-j)\ mod\ 8 = 1 \\ a & (i-j)\ mod\ 8 = 2 \\ ac+b & (i-j)\ mod\ 8 = 3 \\ ab+bc & (i-j)\ mod\ 8 = 4 \\ 1 & (i-j)\ mod\ 8 = 5 \\ a+c & (i-j)\ mod\ 8 = 6 \\ b & (i-j)\ mod\ 8 = 7 \end{cases}, \qquad 0 \le i,j < 8.$$

Construction 6 is merely an example for decomposition of 8×8 matrices. One can search these types of constructions to find matrices P which are MDS.

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

[1] J. Daemen, V. Rijmen, AES proposal: Rijndael. Selected as the Advanced Encryption Standard. Available from http://nist.gov/aes

[2] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Twofish: A 128-bit Block Cipher; 15 June, 1998

[3] P. Ekdahl, T. Johansson, SNOW a new stream cipher, Proceedings of first NESSIE Workshop, Heverlee, Belgium, 2000

[4] Chinese State Bureau of Cryptography Administration, Cryptographic algorithms SMS4 used in wireless LAN products, available at: http://www.oscca.gov.cn/Doc/6/News-1106.htm

[5] D. Feng, X. Feng, W. Zhang, X. Fan and C. Wu, Loiss: A Byte-Oriented Stream Cipher, Available at http://www.eprint.iacr.org-/2010/489.pdf

[6] ETSI/SAGE: Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 128-EIA3 Document 2: ZUC Specification. Version 1.5, 4th January 2011. Tech. rep., ETSI (2011), http://www.gsmworld.com/documents/EEA3-EIA3-ZUC-v1-5.pdf

[7] Praveen Gauravaram, Lars R Knudsen, Krystian Matusiewicz, Florian Mendel, Christian Rechberger, Martin Schläffer, Søren S Thomsen, Grøstl–a SHA-3 candidate, available via http://www.groestl.info/Groestl.pdf

[8] P. Junod, S. Vaudenay, Perfect Diffusion Primitives for Block Ciphers: Building Efficient MDS Matrices, Selected Areas in Cryptography (2004)

[9] M. R. Mirzaee Shamsabad, A. Mahmoodi Rishakani, S. M. Dehnavi, H. Maimani, “Linearized MDS and Almost MDS Diffusion Layers”, 9th International Conference on Information Security and Cryptology (ISCISC’12), University of Tabriz, Tabriz, Iran, 2012 (In Persian)

[10] M. Sadjadieh, M. Dakhilalian, H. Mala, P. Sepehrdad, Recursive Diffusion Layers for Block Ciphers and Hash Functions, FSE’12, USA, 2012

[11] D. Augot, M. Finiasz, Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions, ISIT 2013: 1551-1555

[12] S. M. Dehnavi, A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad, H. Maimani, E. Pasha, Construction of New Families of MDS Diffusion Layers, IACR Cryptology ePrint Archive 2014:011, (2014).

[13] S. M. Dehnavi, A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad, On cryptographic applications of matrices acting on finite commutative rings, IACR Cryptology ePrint Archive 2014:091, (2014).

[14] A. Mahmoodi Rishakani, S. M. Dehnavi, M. R. Mirzaee Shamsabad, Hamidreza Maimani, Einollah Pasha, New concepts in design of lightweight MDS diffusion layers, Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on Cryptography and Information Security.

[15] J. Guo, T. Peyrin, and A. Poschmann, The PHOTON Family of Lightweight Hash Functions, In CRYPTO’11, volume 6841, pages 222–239. Springer-Verlag, 2011.

[16] J. Guo, T. Peyrin, and M. Robshaw, The LED Block Cipher, In CHES’11, volume 6917, pages 326–341. Springer-Verlag, 2011.

[17] San Ling, Chaoping Xing, Coding Theory: A First Course, Cambridge University Press, 2004.

[18] F. J. MacWilliams and N.J.A. Sloane, “The Theory of Error-Correcting Codes”, North-Holland, Amsterdam, 1998.

[19] S. M. Dehnavi, A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad, Bitwise Linear Mappings with Good Cryptographic Properties and Efficient Implementation, IACR Cryptology ePrint Archive 2015: 225 (2015)