Direct Exponent and Scalar Multiplication Classes of an MDS Matrix

Ghulam Murtaza[1], Nassar Ikram[2]

[1,2] National University of Sciences and Technology, Pakistan
[1]azarmurtaza@hotmail.com
[2]dr_nassar_ikram@yahoo.com

Abstract. An MDS matrix is an important building block adopted by different algorithms that provides diffusion and therefore, has been an area of active research. In this paper, we present an idea of direct exponent and direct square of a matrix. We prove that direct square of an MDS matrix results in an MDS matrix whereas direct exponent may not be an MDS matrix. We also delineate direct exponent class and scalar multiplication class of an MDS matrix and determine the number of elements in these classes. In the end, we discuss the standing of design properties of a cryptographic primitive by replacing MDS matrix by dynamic one.

Keywords: Dynamic MDS Matrix, Direct Exponent Matrix, AES, Key Based Diffusion, MDS Matrix Classes.

1 Introduction

According to Shannon, confusion and diffusion are two mandatory properties for a secure cipher [1]. Confusion is to make the relationship of statistical independence between ciphertext string and the statistical independence of plaintext string more complicated while Diffusion is associated with dependency of bits of the output on bits of the input. A cipher with good diffusion satisfies the Strict Avalanche Criteria (SAC), one of the prime requirements for algorithms to meet.

Serge Vaudenay suggested to use MDS matrices in cryptographic primitives to produce multi-permutations [2]. These functions have perfect diffusion i.e. for a change of t input bits out of m bits; at least m-t+1 of the output bits are changed. The branch number of diffusion layer in SPN structure has been regarded as a criterion for diffusion layer design. As MDS matrix can reach maximum branch number compared with permutation of similar size, so it is of good diffusion property.

MDS matrices are used for diffusion in block ciphers like AES [3], Twofish [4] and Khazad [5]. These are also used in stream ciphers like MUGI [6] and cryptographic hash functions like WHIRLPOOL [7].

The use of keyed components in the design of cryptographic algorithms is well known [4, 9, 10. 11, 12, 14, 17]. It is another school of thought in the designing of secure cryptographic primitive. In [4, 9] the author uses keyed S-Boxes having concepts of providing more security over ciphers using fixed S-Boxes. Although there exist some analyses [13] of ciphers that are based on these keyed S-Boxes but still they are not as mature as in case of fixed S-Boxes if used in same cipher. Moreover, multiple layer security approach [17] seems noble in designing cryptographic algorithms by keeping efficiency in view. This approach is used to enhance the security of existing ciphers and can also be used to increase the key size without redesigning a key scheduling algorithm.

In [8], the authors show that scalar multiplication of an MDS Matrix is an MDS Matrix. By using the results, crypto primitives can be designed with keyed MDS layer, instead of using some static MDS layer. In this paper our effort is to classify some methods of generating new MDS Matrices from existing matrices and help crypto primitive designers to introduce dynamic MDS Matrix Layer in their designs.

The rest of the paper is organized as follows. In Section 2, we define a direct square matrix and prove that direct square matrix of an MDS Matrix is also an MDS matrix. In Section 3 we define direct exponent matrix and direct exponent class of MDS Matrices. Section 4 presents the scalar multiplication of MDS Matrix classes. In section 5 we briefly discuss the aspiration behind the use of MDS Matrices in a cipher algorithm and make out that the use of dynamic MDS does not affect the purpose of MDS matrices.

2 Direct Exponent MDS Matrix Class

In this section, we define a direct exponent MDS Matrix Class. We find out the number of MDS matrices in this class. We also have an example of direct exponent MDS Matrix Class in case of AES algorithm. We will explicitly use notation F for field $GF[x]/f(x)$ from now onwards.

Definition 1

If $A = [a_{i,j}]_{mxm}$, we say Direct Exponent (element-wise exponent matrix), A_{d^e} of A is a matrix whose each element is the result of exponentiation of corresponding elements of A. If $e = 2$, then we say A_{d^2} is a direct square matrix of A.

In the following, we prove that direct square of an MDS matrix is an MDS matrix. We will use a well know result about MDS Matrices i.e. A matrix A is an MDS Matrix iff all of its square sub matrix are non singular

Theorem 1

If $A = [a_{i,j}]_{mxm}$, $a_{i,j} \in F$ is an MDS matrix, then direct square matrix A_{d^2} of A is an MDS matrix.

Proof

Let A be an MDS matrix => for any square sub-matrix S of A ,$|S| \neq 0$

=> Rank of S = No of rows of S = No of columns of S

We take any two rows say S'_{R_1}, S'_{R_2} of $S' = S_{d^2} = [s^2_{i,j}]$,

where $1 \leq R_1, R_2 \leq m, R_1 \neq R_2$

We have to show that $S'_{R_1} \neq k.S'_{R_2}$ for any $k \epsilon F$

Suppose that $S'_{R_1} = k.S'_{R_2}$ for some k so that $|S'| = 0$

$$=> s^2_{R_1,j} = k.s^2_{R_2,j} \ \forall \ j$$

$$=> s_{R_1,j} = k'.s_{R_2,j} \ \forall \ j, \text{ where } k'^2 = k \in F$$

$$=> S_{R_1} = k'.S_{R_2}, \text{ for some } k' \in F$$

=> Rank of S < Rows of S

=> A contradiction to that A is an MDS matrix. Hence our supposition is incorrect and A_{d^2} is an MDS matrix.

Corollary 1

If $A = [a_{i,j}]_{mxm}$, $a_{i,j} \in F$ is an MDS matrix, then $A_{d^{2^i}}$, $i = 1,2,...$ of A is an MDS matrix.

The following theorem provides the relation between inverse of an MDS Matrix and inverse of its direct square matrix. It can be used to efficiently compute inverse of direct square of an MDS matrix.

Theorem 2

If inverse of a matrix B is A then inverse of direct square matrix of B is $A_{d^2}{}^{-1}$.

Proof

Let $A = [a_{i,j}]_{mxm}, B = [b_{i,j}]_{mxm}$, $a_{i,j}, b_{i,j} \in GF[x]/f(x)$ and $B = A^{-1} \Rightarrow a_{i,j} . b_{i,j} = 0$ for $i \neq j$ and $a_{i,i} . b_{i,i} = 1$. As $A_{d^2} = [a_{i,j}^2]_{mxm}$ and $B_{d^2} = [b_{i,j}^2]_{mxm}$, so we have $a_{i,j}^2 . b_{i,j}^2 = a_{i,j} . a_{i,j} . b_{i,j} . b_{i,j} = 0$ and $a_{i,i}^2 . b_{i,i}^2 = a_{i,i} . a_{i,i} . b_{i,i} . b_{i,i} = 1$. Hence the proof.

Definition 2

We define direct exponent class of MDS matrix A as $Cl_{d^e}(A) = \{A` : A` = A_{d^i}, i = 2,3,4, \ldots Ord(F)\}$

Theorem 3

If $A = [a_{i,j}]_{mxm}$, $a_{i,j} \in F$ is an MDS matrix, then direct exponent matrix, A_{d^e} of A for $e \neq 2^i$ is not necessarily be an MDS matrix.

Proof

Since for any $k_1, k_2 \in F$. If $k_1^e = k_2^e \Rightarrow k_1 = k_2$, then direct exponent matrix A_{d^e} is not an MDS matrix.

Lemma 1

If $A = [a_{i,j}]_{mxm}$, $a_{i,j} \in F$ is not an MDS matrix, then direct square matrix and direct exponent matrix of A are not MDS matrices.

Proof

Since for any $s_{R_1,j} = k . s_{R_2,j} \Rightarrow s_{R_1,j}^2 = k^i . s_{R_2,j}^2 \; \forall \, i$

Theorem 4

If an element $a^/$ of MDS Matrix A such that $|a^/| = Max|a_{i,j}|$, then $\frac{\log|a^/|}{\log 2} - 1 \leq$ # MDS matrices in $Cl_{d^e}(A) \leq Ord(F) - 1$

Proof

Since by theorem 1, we have $A_{d^i}, i = 2^k, k = 1,2,3, \ldots$ is an MDS matrix, therefore, for an order $|a^/|$, we have at least $\frac{\log|a^/|}{\log 2} - 1$ different MDS matrices. Now as order of any element of matrix may have a maximum value equal to the order of field, so

number of different MDS Matrices generated can not exceeds the $\mathrm{Ord}(F) - 1$. Hence the proof.

Example 1

Direct exponent class of MDS matrix used in AES contains 236 MDS matrices. The matrices generated by the following exponents are not MDS matrices.

13	26	51	52	67	85	102	104	119	134
153	161	170	187	204	208	221	238	255	

3 Scalar Multiplication MDS Matrix Class

In this section, we define a scalar multiplication MDS matrix Class. We find out the number of MDS matrices in this class. We also have an example of number of elements in scalar multiplication MDS matrix of AES algorithm.

Theorem 5

Let $A = [a_{i,j}]_{mxm}$, $a_{i,j} \in F_q$ be an MDS matrix, for an element $e \neq 0 \in F_q$, eA is an MDS matrix [8].

The proof of above result given in [8] is valid for element $e \neq 0 \in F_q$ multiplied to single or more rows of the matrix A. In the following we generalize this result for elements $e_i \neq 0 \in F_q, i = 1,2, \dots, m$, multiplying $i - \text{th}$ row of matrix A where e_k not necessarily be the same as e_l for any $1 \leq k, l \leq m$.

Theorem 6s

Let $A = \begin{bmatrix} A_1 \\ \vdots \\ A_m \end{bmatrix}, A_i = [\, a_{i,1} \quad \cdots \quad a_{i,n}]$, $a_{i,j} \in F_q$ be an MDS matrix, and $E = [\, e_i], i = 1,2, \dots, m.$ then scalar multiplication $EA = \begin{bmatrix} e_1 A_1 \\ \vdots \\ e_m A_m \end{bmatrix}$, $e_i A_i = [\, e_i\, a_{i,1} \quad \cdots \quad e_i\, a_{i,n}]$ is an MDS Matrix.

Proof

We prove the result on the same ground as of theorem 5 given in [8].

Let $A_{m\times n}$ be an MDS matrix $\Rightarrow$ any sub square matrix $S_{l\times l}$ of $A_{m\times n}$, $1 \le l \le \min(m,n)$, $|S_{l\times l}| \neq 0$.

Suppose EA is not an MDS matrix $\Rightarrow \exists\ E_l\ S_{l\times l}, E_l = \begin{bmatrix} e_{k_1} \\ \vdots \\ e_{k_l} \end{bmatrix}, 1 \le k_1, \dots, k_l \le \min(m,n)$ such that $|E_l\ S_{l\times l}| = 0 \Rightarrow E_l|\ S_{l\times l}| = 0 \Rightarrow |\ S_{l\times l}| = 0\ \because e_i \neq 0\ \forall i$, a contradiction to that $A_{m\times n}$ is an MDS matrix. So our supposition that EA is not an MDS matrix is wrong.

Definition 3

We define scalar multiplication class of an MDS matrix $\grave{A}_{m\times n}$ by a scalar value $E = \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix}$ as $Cl_{sm}(A_{m\times n}) = \{\grave{A}_{m\times n} : \grave{A}_{m\times n} = E\ A_{m\times n}, \forall e_i \neq 0 \in F, \forall i\}$

Theorem 6

Number of elements in class $Cl_{sm}(\grave{A}_{m\times n})$ is $(Ord(F)-1)^m$.

Proof

Clearly the non-zero number of elements in field F is $Ord(F)-1$. Since there are m such elements in E so number of elements in class is $(Ord(F)-1)\times(Ord(F)-1)\times \dots m-times = (Ord(F)-1)^m$.

Example 2

For MDS matrix used in AES, the number of elements for which newly generated matrices are MDS one, would be $(2^8-1)^4 \cong 2^{31.25}$.

4 Viability of Use in Crypto Primitives

Generally in the design of crypto primitives, an MDS matrix is used as a part of its diffusion component. In some ciphers like AES, it is also used to maximize the number of active S-Boxes which provides immunity against differential cryptanalysis. The quantitative effect of an MDS Matrix with the change proposed is independent of the coefficients of MDS Matrix used. Furthermore, changing the coefficients of MDS Matrix, the resultant cipher is isomorphic [16] to the original. Therefore it is obvious that there is no difference in statistical properties of cipher by changing its MDS

Matrix. Similarly the design strength of a crypto primitive remains unaltered using different MDS matrices.

5 Conclusion

We have defined direct square of a matrix and showed that direct square of an MDS matrix is an MDS matrix. We can use this method to generate a random MDS matrix from the existing one. We also present direct exponent class and scalar multiplication class of an MDS matrix. Our work is helpful in designing ciphers with keyed MDS matrices. It will also open ways in describing diffusion switching mechanism in ciphers containing MDS layers and possible cryptanalytic techniques based on it. Moreover the strength of primitive against different cryptanalytic techniques can be enhanced by introducing dynamic MDS matrices using these classes in perspective of multiple layered security[17].

References

1. Shannon, C.: Communication Theory of Secrecy Systems, Bell System Technical Journal, 28(4), pp. 656--715 (1949), http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf
2. Vaudenay, S.: On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER, FSE, Second International Workshop Proceedings, pp. 286--297, Springer Verlag (1995).
3. Daemen, J., Rijmen, V.: The design of Rijndael: AES, The Advanced Encryption Standard. Springer Verlag (2002).
4. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., Ferguson, N.: Twofish: A 128-bit block cipher (1998). http://www.counterpane.com/twofish.html
5. Barreto, P., Rijmen, V.: The Khazad: legacy-level block cipher. First open NESSIE Workshop, pp. 13--14, Leuven (2000).
6. Watanabe, D., Furuya, S., Yoshida, H., Takaragi, K., Preneel, B.: A New Keystream Generator MUGI. In Revised Papers, vol 2365, LNCS, pp 179–194, Heidelberg, B., Springer Verlag (2002).
7. Barreto, P. S. L. M., Rijmen, V.: The Whirlpool hashing function: Primitive submitted to NESSIE, Sept. 2000. Available at http://www.cryptonessie.org/
8. Murtaza, G., Ikram, N.: New Methods of Generating MDS Matrices. In: Proceedings of ICWC 2008, pp 129-133, ISBN: 978-983-44069, Kuala Lumpur, (2008).
9. Kazys, K., Jaunius, K.: Key-Dependent S-Box Generation in AES Block Cipher System. INFORMATICA, vol. 20, No. 1 pp 23–34 (2009).
10. Sklavos, N., Koufopavlou, O.: Data dependent rotations, a trustworthy approach for future encryption systems/ciphers: low cost and high performance. Computers & Security Vol 22, No 7.
11. Davood, R. P., Mohamad, R.M.S., Kamel, A.M.A., Mohamed, O.: The New Variable-Length Key Symmetric Cryptosystem. JMS, vol. 5, No. 1 pp 24-31, ISSN 1549-3644, (2009).
12. Haitner, I., Holenstein, T.: On the (im)possibility of key dependent encryption. In Proc. of TCC '09, LNCS 5444, pp. 202-219. Springer Verlag (2008).

13. Murphy, S., Robshaw, M.: Key dependent S-Boxes, Differential Cryptanalysis and Twofish, (2002).
14. Alvarez, G., Guia, D., Montoya, F., Peinado, A.: Akelarre: A New Block Cipher Algorithm," SAC '96, pp. 1-14 Kingston, Ontario, (1996).
15. Ferguson, N., Schneier, B.: Cryptanalysis of Akelarre," SAC '97, pp. 201-212 School of Computer Science, Carleton University, (1997).
16. Barken, E., Biham, E.: In how many ways can you write Rijndael? LNCS, vol. 2501, pp 160-175, ASIACRYPT (2002).
17. Borst, J.: The bolck cipher: Grand Cru, Available at https://www.cosic.esat.kuleuven.be/nessie/workshop/submissions/grandcru.zip