Towards a General Construction of Recursive MDS Diffusion Layers

Kishan Chand Gupta, Sumit Kumar Pandey, Ayineedi Venkateswarlu

Towards a General Construction of Recursive MDS Diffusion Layers
(Extended Abstract)

Kishan Chand Gupta[1], Sumit Kumar Pandey[2], and Ayineedi Venkateswarlu[3]

[1] Applied Statistics Unit, Indian Statistical Institute,
203, B.T. Road, Kolkata-700108, INDIA.
kishan@isical.ac.in
[2] C.R. RAO AIMSCS, University of Hyderabad Campus,
Prof. C.R. Rao Road, Hyderabad - 500046, INDIA.
emailpandey@gmail.com
[3] Computer Science Unit, Indian Statistical Institute - Chennai Centre,
MGR Knowledge City Road, Taramani, Chennai - 600113, INDIA.
venku@isichennai.res.in

Abstract. MDS matrices are of great importance in the design of block ciphers and hash functions. MDS matrices are in general not sparse and have a large description and thus induces costly implementation in software/hardware. To overcome this problem, in particular for applications in light-weight cryptography, it was proposed by Guo *et. al.* to use recursive MDS matrices. Such matrices can be computed as a power of companion matrices. Following this, some ad-hoc techniques are proposed to find recursive MDS matrices which are suitable for hardware/software implementation. In another direction, coding theoretic techniques are used to directly construct recursive MDS matrices: Berger technique uses Gabidulin codes and Augot et. al. technique uses shortened BCH codes. In this paper, we provide a necessary and sufficient condition to construct recursive MDS matrices from non-singular diagonable companion matrices. Then we provide three methods to construct recursive MDS matrices. Moreover, recursive MDS matrices obtained through our first method are same as those obtained using shortened BCH codes. The other two methods provide those companion matrices which can be obtained from Gabidulin codes. However, our formulation of necessary and sufficient condition provides many more possibilities to explore to get recursive MDS matrices.

Keywords: Companion matrix, Recursive MDS matrix, Shortened BCH code, Gabidulin code.

1 Introduction

Confusion and Diffusion [26] are two essential properties required to design block ciphers and hash functions. The concept of multipermutation [25, 28] is one possibility of formalizing the notion of perfect diffusion. Another way to formalize

the notion of perfect diffusion is by using Maximum Distance Seperable (MDS) codes. MDS [18, 16] matrices provide high branch number [7] which means a small change in the input will change output bits a lot. Many block ciphers like AES [9], Twofish [23, 24], SHARK [21], Square [8], Khazad [6], Clefia [27], MDS-AES [20] etc. use MDS matrices in their diffusion layers. Such matrices also play an important role in the design of many hash functions like Maelstrom [10], Grϕstl [12] and PHOTON family [13].

A common approach to implement MDS diffusion layers in many ciphers is to use pre-computed tables, but this may not be suitable for resource constrained environments. Several other techniques have also been used like circulant or modification of circulant like matrix to obtain simpler MDS matrix, as in AES [9] and FOX [17]. Another method proposed recently, particularly for resource constrained environments, is to use recursive MDS matrices, known examples that employ such matrices are PHOTON family of hash functions [13] and LED block cipher [14]. A recursive MDS matrix of size n is an MDS matrix which can as obtained as a power of a simple companion matrix (see Definition 2) of size n. The main advantage of this approach is that it can be efficiently implemented in hardware using LFSRs where the last row (or column) of the companion matrix gives the connection polynomial of LFSR. Following the work of Guo et. al [13], some recent papers [22, 15, 4, 30, 1–3] study the construction of efficient recursive MDS matrices.

In Indocrypt 2013, Berger [4] proposed a method to construct recursive MDS matrices from Gabidulin Codes [5]. This construction produces not only an MDS matrix but an MRD (Maximum Rank Distance) [11] matrix also. Then in FSE 2014, Augot and Finiasz [2, 3], gave another construction of recursive MDS matrices using shortened BCH codes. In this method, first a generating polynomial $g(x)$ for BCH code over $\mathbb{F}_q$ is computed with suitable parameters. For such a BCH code to be an MDS code, it is required that $g(x)$ must belong to $\mathbb{F}_q[x]$. Once a MDS BCH code is obtained, it is shortened to get to get a recursive MDS matrix. It is equal to a power of the companion matrix associated with the generating polynomial $g(x)$ of the MDS BCH code.

Our Contribution : We provide a necessary and sufficient condition for a non-singular diagonable companion matrix to produce an MDS matrix when it is raised to some power. We also present three methods - I, II(a) and II(b) derived from the necessary and sufficient conditions to construct non-singular diagonable companion matrix which can be used to produce MDS matrix by raising it to some power. Out of these constructions, first one (I) gives the companion matrices that can be obtained from shortened BCH code whereas II(a) & II(b) give the companion matrices which can be obtained through Gabidulin codes. However, our formulation of necessary and sufficient condition provides many more possibilities to construct companion matrices yielding recursive MDS matrices.

2 Preliminaries

Throughout this paper let $\mathbb{F}_q$ denote the field containing q elements for some prime power q and let $\mathbb{F}_q[x]$ denote the polynomial ring over $\mathbb{F}_q$ in the variable x. It is assumed that the characteristic of $\mathbb{F}_q$ is $char(\mathbb{F}_q) = p$ for some prime p unless otherwise mentioned, which means $q = p^s$ for some positive integer s. Let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{F}_q[x]$ and $a_n \neq 0$. Then the degree of f is n and we denote it as $\deg(f)$. The polynomial f is said to *monic* if its leading coefficient $a_n = 1$.

Definition 1. *Let γ be an element in some extension of $\mathbb{F}_q$. The* minimal polynomial *of γ over $\mathbb{F}_q$, denoted by $\mathrm{Min}_{\mathbb{F}_q}(\gamma)$, is the lowest degree monic polynomial $\mu(x)$ with coefficients from $\mathbb{F}_q$ such that $\mu(\gamma) = 0$.*

Let $\mathcal{M}_{m\times n}(\mathbb{F}_q)$ denote the set of all matrices of size $m \times n$ over $\mathbb{F}_q$. For simplicity, we use $\mathcal{M}_n(\mathbb{F}_q)$ to denote the ring of all $n \times n$ matrices (square matrices of order n) over $\mathbb{F}_q$. Let I_n denote the identity matrix of $\mathcal{M}_n(\mathbb{F}_q)$. The determinant of a matrix $A \in \mathcal{M}_n(\mathbb{F}_q)$ is denoted by $\det(A)$. A square matrix A is said to be non-singular if $\det(A) \neq 0$ or equivalently, the rows (columns) of A are linearly independent over $\mathbb{F}_q$.

Definition 2. *Let $f(x) = a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$ be a monic polynomial over $\mathbb{F}_q$ of degree n. The* companion matrix *$C_f \in \mathcal{M}_n(\mathbb{F}_q)$ associated to the polynomial f is given by*

$$C_g = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & 1 \\ -a_0 & -a_1 & \dots & \dots & -a_{n-1} \end{pmatrix}.$$

We sometimes use the notation $\mathsf{Companion}(a_0, a_1, \dots, a_{n-1})$ to represent the companion matrix C_f.

Definition 3. *A matrix $D = (\lambda_{i,j}) \in \mathcal{M}_n(\mathbb{F}_q)$ is said to be* diagonal *if $\lambda_{i,j} = 0$ for $i \neq j$.*

By setting $\lambda_i = \lambda_{i,i}$, we denote the diagonal matrix D as $diag[\lambda_1, \lambda_2, \dots, \lambda_n]$. It is obvious to see that the determinant of D is $\det(D) = \prod_{i=1}^{n} \lambda_i$. Hence the diagonal matrix D is non-singular if and only if $\lambda_i \neq 0$ for all $i = 1, \dots, n$.

Definition 4. *A matrix $V \in \mathcal{M}_n(\mathbb{F}_q)$ is called Vandermonde matrix if it is represented as*

$$V = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \cdots & \lambda_{n-1} & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \cdots & \lambda_{n-1}^2 & \lambda_n^2 \\ \lambda_1^3 & \lambda_2^3 & \lambda_3^3 & \cdots & \lambda_{n-1}^3 & \lambda_n^3 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \lambda_1^{n-2} & \lambda_2^{n-2} & \lambda_3^{n-2} & \cdots & \lambda_{n-1}^{n-2} & \lambda_n^{n-2} \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \lambda_3^{n-1} & \cdots & \lambda_{n-1}^{n-1} & \lambda_n^{n-1} \end{bmatrix},$$

where $\lambda_i \in \mathbb{F}_q$ for $i = 1, \ldots, n$. We use the notation $vand[\lambda_1, \lambda_2, \ldots, \lambda_n]$ to denote the Vandermonde matrix V. It is well-known that the determinant of V is given by $\det(V) = \prod_{1 \le i < j \le n}(\lambda_j - \lambda_i)$, and so the matrix V is non-singular if and only if $\lambda_i \neq \lambda_j$ for all $1 \le i < j \le n$.

Definition 5. *A matrix $GV \in \mathcal{M}_n(\mathbb{F}_q)$ of order n is called generalized Vandermonde matrix if it is represented as*

$$GV = \begin{bmatrix} \lambda_1^{r_1} & \lambda_2^{r_1} & \lambda_3^{r_1} & \cdots & \lambda_{n-1}^{r_1} & \lambda_n^{r_1} \\ \lambda_1^{r_2} & \lambda_2^{r_2} & \lambda_3^{r_2} & \cdots & \lambda_{n-1}^{r_2} & \lambda_n^{r_2} \\ \lambda_1^{r_3} & \lambda_2^{r_3} & \lambda_3^{r_3} & \cdots & \lambda_{n-1}^{r_3} & \lambda_n^{r_3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \lambda_1^{r_{n-1}} & \lambda_2^{r_{n-1}} & \lambda_3^{r_{n-1}} & \cdots & \lambda_{n-1}^{r_{n-1}} & \lambda_n^{r_{n-1}} \\ \lambda_1^{r_n} & \lambda_2^{r_n} & \lambda_3^{r_n} & \cdots & \lambda_{n-1}^{r_n} & \lambda_n^{r_n} \end{bmatrix}$$

where $\lambda_i \in \mathbb{F}_q$ for $i = 1, \ldots, n$ and $0 \le r_1 < r_2 < \cdots < r_n$. We denote the generalized Vandermonde matrix GV by $genvand[\lambda_1, \lambda_2, \ldots, \lambda_n; r_1, r_2, \ldots, r_n]$. A Vandermonde matrix is a special case of the generalized Vandermonde matrix where $r_1 = 0$ and $r_i = r_{i-1} + 1$ for $i = 2, \ldots, n$. The calculation of determinant of generalized Vandermonde matrix is not straightforward; see [19] for details.

Definition 6. *Let $\theta : x \mapsto M \times x$ be a mapping from $\mathbb{F}_q^m$ to $\mathbb{F}_q^n$ defined by $M \in \mathcal{M}_{m \times n}(\mathbb{F}_q)$. The matrix M is said to be MDS matrix if the set $(x, M \times x)$ is an MDS code,* i.e.*, a linear code of dimension m, length $m + n$ and minimal distance $n + 1$.*

We are interested in only square MDS matrices, i.e., $m = n$, as the input and output of diffusion layer are of same size. The following facts can be used to characterize MDS matrices.

Fact 1: A matrix $M \in \mathcal{M}_n(\mathbb{F}_q)$ is MDS if and only if all its square submatrices are non-singular.
Fact 2: A matrix $M \in \mathcal{M}_n(\mathbb{F}_q)$ is MDS if and only if any n rows of the matrix $\left[\frac{I_n}{M}\right]$ are linearly independent.

Definition 7. *A matrix $M \in \mathcal{M}_n(\mathbb{F}_q)$ of order n is diagonable if there exists a diagonal matrix D and a non-singular matrix P such that $M = PDP^{-1}$.*

Lemma 1. *Let $C = \mathsf{Companion}(z_0, z_1, \cdots, z_{n-1}) \in \mathcal{M}_n(\mathbb{F}_q)$ be a non-singular companion matrix which is diagonable, say $C = PDP^{-1}$ where P is an $n \times n$ non-singular matrix and $D = diag[\lambda_1, \lambda_2, \ldots, \lambda_n]$. Then all entries of P will be non-zero. Moreover, C can be expressed as VDV^{-1} where $V = vand[\lambda_1, \lambda_2, \cdots, \lambda_n]$.*

Proof. If C is a non-singular matrix then all λ_i's will be non-zero. Now, let $P = [\boldsymbol{v}_1\ \boldsymbol{v}_2\ \ldots\ \boldsymbol{v}_n]$ where $\boldsymbol{v}_i$'s are represented as $n \times 1$ column vector. Then $CP = PD$ and hence $C\boldsymbol{v}_i = \lambda_i \boldsymbol{v}_i$ for all $i = 1, \ldots, n$. (in other words, $\boldsymbol{v}_i$'s are eigenvectors of C corresponding to eigenvalue λ_i). Then,

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -z_0 & -z_1 & -z_2 & \cdots & -z_{n-1} \end{bmatrix} \begin{bmatrix} v_{i,1} \\ v_{i,2} \\ \vdots \\ v_{i,n-1} \\ v_{i,n} \end{bmatrix} = \lambda_i \begin{bmatrix} v_{i,1} \\ v_{i,2} \\ \vdots \\ v_{i,n-1} \\ v_{i,n} \end{bmatrix}$$

where $\boldsymbol{v}_i = [v_{i,1}\ v_{i,2}\ \cdots\ v_{i,n}]^T$. From the above identity, we get

$$v_{i,2} = \lambda_i v_{i,1}\ ;\quad v_{i,3} = \lambda_i v_{i,2}\ ;\quad \cdots\ ;\quad v_{i,n} = \lambda_i v_{i,n-1} \tag{1}$$

Since λ_i's are non-zero, hence for all $i = 1, \cdots, n$ and for all $j = 1, \cdots, n$, $v_{i,j}$'s also will be non-zero. From equation (1), it is clear that $v_{i,j} = \lambda_i^{j-1} v_{i,1}$ and hence $P = VD'$ where,

$$V = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \cdots & \lambda_n^2 \\ \vdots & \vdots & & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \cdots & \lambda_n^{n-1} \end{bmatrix}; D' = \begin{bmatrix} v_{1,1} & 0 & \cdots & 0 \\ 0 & v_{2,1} & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & v_{n,1} \end{bmatrix}$$

So, $C = PDP^{-1} = VD'DD'^{-1}V^{-1} = VDV^{-1}$. Hence, the lemma. □

Corollary 1. *A companion matrix C is non-singular and diagonable if and only if all eigenvalues of C are distinct and non-zero.*

Proof. If all eigenvalues of C are non-zero then C is non-singular. If all eigenvalues of C are distinct then it is diagonable. Hence, if all eigenvalues of C are distinct and non-zero then C is non-singular and diagonable.

Conversely, let C is non-singular, then all its eigenvalues are non-zero. Now, let companion matrix C is diagonable. Then $C = VDV^{-1}$ (from Lemma 1) where $V = vand[\lambda_1, \lambda_2, \cdots, \lambda_n]$, $D = diag[\lambda_1, \lambda_2, \cdots, \lambda_n]$ and λ_is are eigenvalues of C. For V^{-1} to exist, it is required that λ_i's must be distinct. Hence if companion matrix C is non-singular and diagonable, all its eigenvalues are distinct and non-zero. □

Remark 1. We can also have an analogous result for non-diagonable companion matrices similar to Lemma 1. In this case we need to deal with *confluent* Vandemonde matrices.

3 Necessary and Sufficient Condition for Constructing Recursive MDS matrix

In this section, we prove a necessary and sufficient condition to construct MDS matrix recursively from non-singular diagonable companion matrix. Let C be a companion matrix in $\mathcal{M}_n(\mathbb{F}_q)$ of order n. If C^k is MDS for some $k > 0$, then

C must be non-singular. For the proposed necessary and sufficient condition, we assume one more property on C - diagonable. As mentioned in the above remark, the case of non-diagonable matrices can be dealt with similarly. In such a case we can work with Jordan form of the companion matrix and confluent Vandermonde matrix containing the generalized eigenvectors. In fact, it can be shown that recursive MDS matrices over binary extension fields can only be obtained from diagonable companion matrices. We will give the detailed proofs in the general case in the full version of the paper.

Now we state necessary and sufficient condition to construct recursive MDS matrices.

Theorem 1. *Let $C \in \mathcal{M}_n(\mathbb{F}_q)$ be a non-singular diagonable companion matrix, i.e., $C = VDV^{-1}$ where $D = diag[\lambda_1, \lambda_2, \cdots, \lambda_n]$ and $V = vand[\lambda_1, \lambda_2, \cdots, \lambda_n]$. Then C^k, $k \geq n$, is MDS if and only if $genvand[\lambda_1, \lambda_2, \cdots, \lambda_n; r_1, r_2, \cdots, r_n]$ is non-singular for all $\{r_1, r_2, \cdots, r_n\} \subseteq \{0, 1, 2, \ldots, n-1, k, k+1, \cdots, k+n-1\}$.*

Proof. If C is an $n \times n$ companion matrix, then it is easy to check that C^k can not be MDS if $k < n$. Hence $k \geq n$. We have $C = VDV^{-1}$ which implies $C^k = VD^kV^{-1}$ where $D^k = diag[\lambda_1^k, \lambda_2^k, \cdots, \lambda_n^k]$. Let

$$\bar{V} = VD^k = \begin{bmatrix} \lambda_1^k & \lambda_2^k & \cdots & \lambda_n^k \\ \lambda_1^{k+1} & \lambda_2^{k+1} & \cdots & \lambda_n^{k+1} \\ \vdots & \vdots & & \vdots \\ \lambda_1^{k+n-1} & \lambda_2^{k+n-1} & \cdots & \lambda_n^{k+n-1} \end{bmatrix}$$

so $C^k = VD^kV^{-1} = \bar{V}V^{-1}$.

Consider the $2n \times n$ matrix

$$M = \left[\frac{I_n}{C^k}\right] = \left[\frac{I_n}{\bar{V}V^{-1}}\right]$$

and we can see that C^k is MDS if and only if any n rows of M are linearly independent. Let $1 \leq i_1 < i_2 < \cdots < i_n \leq 2n$ be the indices of n rows chosen from M and let the matrix formed by the chosen rows be A. Let l_1 be the number of rows chosen from $I_{n\times n}$ indexed by $i_1, i_2, \cdots, i_{l_1}$ and l_2 be the number of rows chosen from $\bar{V}V^{-1}$ indexed by $i_{l_1+1}, i_{l_1+2}, \cdots, i_{l_1+l_2}$ such that $0 \leq l_1, 0 \leq l_2$; $l_1 + l_2 = n$; $1 \leq i_1 < i_2 < \cdots < i_{l_1} \leq n$ and $n+1 \leq i_{l_1+1} < i_{l_1+2} < \cdots < i_{l_1+l_2} = i_n \leq 2n$. Let $S = \{i_1, i_2, \cdots, i_n\}$ and

$$A = M_{|S} = \left[\frac{I_n}{\bar{V}V^{-1}}\right]_{|S} = \left[\frac{V}{\bar{V}}\right]_{|S} V^{-1} = A'V^{-1}$$

We can now see that the matrix A is non-singular if and only if the matrix $A' = genvand[\lambda_1, \lambda_2, \cdots, \lambda_n; i_1 - 1, \cdots, i_{l_1} - 1, k + i_{l_1+1} - (n+1), \cdots, k + i_n - (n+1)]$

is non-singular. We have

$$A' = \begin{bmatrix} \lambda_1^{i_1-1} & \lambda_2^{i_1-1} & \cdots & \lambda_n^{i_1-1} \\ \vdots & \vdots & & \vdots \\ \lambda_1^{i_{l_1}-1} & \lambda_2^{i_{l_1}-1} & \cdots & \lambda_n^{i_{l_1}-1} \\ \lambda_1^{k+i_{l_1+1}-(n+1)} & \lambda_2^{k+i_{l_1+1}-(n+1)} & \cdots & \lambda_n^{k+i_{l_1+1}-(n+1)} \\ \vdots & \vdots & & \vdots \\ \lambda_1^{k+i_n-(n+1)} & \lambda_2^{k+i_n-(n+1)} & \cdots & \lambda_n^{k+i_n-(n+1)} \end{bmatrix}$$

Let $i_1-1 = r_1, \cdots, i_{l_1}-1 = r_{l_1}, k+i_{l_1+1}-(n+1) = r_{l_1+1}, \cdots, k+i_n-(n+1) = r_n$. Since $k \geq n$ and $1 \leq i_1 < i_2 < \cdots < i_n \leq 2n$, hence $r_1 < \cdots < r_{l_1} < r_{l_1+1} < \cdots < r_n$ and $\{r_1, \cdots, r_n\} \subseteq \{0, 1, 2, \cdots, n-1, k, k+1, k+n-1\}$. Hence the proof. □

Remark 2. The polynomial associated to the companion matrix C is given by $g = \prod_{i=1}^{n}(x - \lambda_i) \in \mathbb{F}_q[x]$. The necessary and sufficient condition is equivalent to saying that the polynomial f has no multiple of the form $m_0 + m_1 x + \cdots + m_{n-1}x^{n-1} + m_k x^k + \cdots + m_{n+k-1}x^{n+k-1}$ of weight $\leq n$. These results can also be extended to the case of non-diagonable matrices.

Now we provide three constructions of companion matrices by which recursive MDS matrices can be obtained. In the following we let $C \in \mathcal{M}_n(\mathbb{F}_q)$ be an $n \times n$ non-singular companion matrix which is diagonable, i.e., $C = VDV^{-1}$ where $D = diag[\lambda_1, \lambda_2, \cdots, \lambda_n]$ and $V = vand[\lambda_1, \lambda_2, \cdots, \lambda_n]$. The polynomial associated to the companion matrix C is given by $g = \prod_{i=1}^{n}(x - \lambda_i) \in \mathbb{F}_q[x]$.

Remark 3. Note that if the polynomial $g = \prod_{i=1}^{n}(x - \lambda_i) \in \mathbb{F}_q[x]$ yields a recursive MDS matrix then for any $\alpha \in \mathbb{F}_q^*$, the polynomial $g_\alpha = \prod_{i=1}^{n}(x - \alpha\lambda_i) \in \mathbb{F}_q[x]$ also yields a recursive MDS matrix.

3.1 Construction - I

We start with the first construction of companion matrix whose eigenvalues are consecutive in powers.

Theorem 2. *Let $\lambda_i = c^{i-1}\lambda_1$, $i = 1, \cdots, n$, be such that $g(x) = \prod_{i=1}^{n}(x - \lambda_i) \in \mathbb{F}_q[x]$. Then C^k, $k \geq n$, is MDS if and only if $c, c^2, \ldots, c^{n-1}, c^k, \ldots, c^{k+n-1}$ are distinct and not equal to 1.*

Proof. From Theorem 1, we can see that the matrix C^k is MDS if and only if $A' = genvand[\lambda_1, \cdots, \lambda_n; r_1, r_2, \cdots, r_n]$ is non-singular for all $\{r_1, r_2, \cdots, r_n\} \subseteq \{0, 1, \cdots, n-1, k, k+1, \cdots, k+n-1\}$. We have $\lambda_i = c^{i-1}\lambda_1$ for $i = 1, \cdots, n$, so $A' = genvand[\lambda_1, c\lambda_1, c^2\lambda_1, \cdots, c^{n-1}\lambda_1; r_1, r_2, \cdots, r_n]$. So we get

$$A' = \begin{bmatrix} \lambda_1^{r_1} & (c\lambda_1)^{r_1} & \cdots & (c^{n-1}\lambda_1)^{r_1} \\ \lambda_1^{r_2} & (c\lambda_1)^{r_2} & \cdots & (c^{n-1}\lambda_1)^{r_2} \\ \vdots & \vdots & & \vdots \\ \lambda_1^{r_n} & (c\lambda_1)^{r_n} & \cdots & (c^{n-1}\lambda_1)^{r_n} \end{bmatrix} = \begin{bmatrix} \lambda_1^{r_1} & (\lambda_1)^{r_1}(c^{r_1}) & \cdots & (\lambda_1)^{r_1}(c^{r_1})^{n-1} \\ \lambda_1^{r_2} & (\lambda_1)^{r_2}(c^{r_2}) & \cdots & (\lambda_1)^{r_2}(c^{r_2})^{n-1} \\ \vdots & \vdots & & \vdots \\ \lambda_1^{r_n} & (\lambda_1)^{r_n}(c^{r_n}) & \cdots & (\lambda_1)^{r_n}(c^{r_n})^{n-1} \end{bmatrix}$$

Let $y_{r_1} = c^{r_1}, y_{r_2} = c^{r_2}, \cdots, y_{r_n} = c^{r_n}$, then $\det(A') = (\prod_{j=1}^{n} \lambda_1^{r_j}) \det(A'')$, where

$$A'' = \begin{bmatrix} 1 & y_{r_1} & y_{r_1}^2 & \cdots & y_{r_1}^{n-1} \\ 1 & y_{r_2} & y_{r_2}^2 & \cdots & y_{r_2}^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & y_{r_n} & y_{r_n}^2 & \cdots & y_{r_n}^{n-1} \end{bmatrix}$$

We have $\lambda_1 \neq 0$ and so $\det(A') \neq 0$ if and only if $\det(A'') \neq 0$. Note that $A'' = vand[y_{r_1}, y_{r_2}, \cdots, y_{r_n}]$ and so $\det(A'') \neq 0$ if and only if $y_{r_1} \neq y_{r_2} \neq \cdots \neq y_{r_n}$ or $c^{r_1} \neq c^{r_2} \neq \cdots \neq c^{r_n}$ for all $\{r_1, r_2, \cdots, r_n\} \subseteq \{0, 1, \cdots, n-1, k, k+1, \cdots, k+n-1\}$ which implies that $1 \neq c \neq c^2 \neq c^3 \neq \cdots \neq c^{n-1} \neq c^k \neq c^{k+1} \neq \cdots \neq c^{k+n-1}$. Hence the proof. □

Relationship with [2]: Augot et. al. proposed a recursive MDS construction using shortened BCH code. First, a generator polynomial $g(x)$ of a BCH code with suitable parameter choices is obtained. The roots of $g(x)$ are non-zero and consecutive in powers, say $\beta^l, \beta^{l+1}, \cdots, \beta^{l+n-1}$. These roots must be conjugate to each other, i.e., $g(x) \in \mathbb{F}_q[x]$, to ensure that $g(x)$ generates a BCH code which is also MDS. Then this code is finally shortened to get a recursive MDS matrix that is a power of the companion matrix associated to the polynomial $g(x)$. Our proposed construction - I yields the same kind of companion matrices. If we take $\lambda_1 = \beta^l \in \mathbb{F}_{p^m}$ and $c = \beta \in \mathbb{F}_{p^m}$, then $\lambda_i = \beta^{l+i-1}$ for $i = 1, \cdots, n$ which are exactly the roots of the generating polynomial $g(x)$.

The above theorem is true for any field and any $k \geq n$. In the next two subsections, we provide two constructions of companion matrices but with some restrictions - (a) the characteristic $\mathbb{F}_q$ is equal to 2 and (b) $k = n$. *These two constructions appear to be similar (but not same)* and hence we denote them by II(a) and II(b).

3.2 Construction - II(a)

Theorem 3. *Let λ_1 and c be in some extension of $\mathbb{F}_q$ and let $\lambda_i = c^{2^{i-2}} \lambda_1$ for $i = 2, \ldots, n$. Then C^n will be an MDS matrix if $deg(Min_{\mathbb{F}_2}(c)) \geq 2n$, where $Min_{\mathbb{F}_2}(c)$ is the minimal polynomial of c over $\mathbb{F}_2$.*

Proof. The proof goes along in the same way as it is in Theorem 2. We get,

$$A'' = \begin{bmatrix} 1 & y_{r_1} & y_{r_1}^2 & y_{r_1}^{2^2} & \cdots & y_{r_1}^{2^{n-2}} \\ 1 & y_{r_2} & y_{r_2}^2 & y_{r_2}^{2^2} & \cdots & y_{r_2}^{2^{n-2}} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & y_{r_n} & y_{r_n}^2 & y_{r_n}^{2^2} & \cdots & y_{r_n}^{2^{n-2}} \end{bmatrix}$$

where $y_{r_1} = c^{r_1}, y_{r_2} = c^{r_2}, \cdots, y_{r_n} = c^{r_n}$. Let,
$P_2 = \prod_{r_1 \leq j_1 < j_2 \leq r_n} (y_{j_1} + y_{j_2})$; $P_4 = \prod_{r_1 \leq j_1 < j_2 < j_3 < j_4 \leq r_n} (y_{j_1} + y_{j_2} + y_{j_3} + y_{j_4})$

$\vdots$

$P_n = (y_{r_1} + y_{r_2} + \cdots + y_{r_n})$ if n is even, else

$P_{n-1} = \prod_{r_1 \leq j_1 < j_2 < j_3 < \cdots < j_{n-1} \leq r_n} (y_{j_1} + y_{j_2} + y_{j_3} + \cdots + y_{j_{n-1}})$.

Then $\det(A'') = P_2 P_4 \cdots P_n$ if n is even otherwise $\det(A'') = P_2 P_4 \cdots P_{n-1}$. From Theorem 1, we can see that the matrix C^n is MDS if and only if $\det(A'') \neq 0$ for all $\{r_1, r_2, \cdots, r_n\} \subseteq \{0, 1, 2, \cdots, n-1, n, n+1, \cdots, 2n-1\}$. Maximum degree of any irreducible term in any P_i can be at most $2n-1$. If $deg(M(c)) \geq 2n$, then none of P_i's will be zero and hence $\det(A'')$ will be non-zero. Thus C^n is an MDS matrix if $deg(M(c)) \geq 2n$ when $\lambda_i = c^{2^{i-2}} \lambda_1$ for $i = 2, \cdots, n$. Hence the proof. □

In the above theorem if $(deg(M(c)) \geq 2n$ then the elements λ_i for $i = 1, \ldots, n$ are linearly independent. So this construction can be seen as similar to the construction discussed in [4, Section 3.2].

3.3 Construction - II(b)

In this subsection, we provide another construction of companion matrices whose eigenvalues' powers are in geometric progression. We then show that the construction proposed in Section 3.4 of [4] gives exactly the same kind of companion matrices.

Theorem 4. *Let λ be in an extension of $\mathbb{F}_q$ and let $\lambda_i = \lambda^{2^{i-1}}$ for $i = 1, \cdots, n$. Then the matrix C^n is MDS if $deg(\mathrm{Min}_{\mathbb{F}_2}(\lambda)) \geq 2n$, where $\mathrm{Min}_{\mathbb{F}_2}(\lambda)$ is the minimal polynomial of λ over $\mathbb{F}_2$.*

Proof. The proof goes along in the same way as it is in Theorem 2. We get,

$$A'' = \begin{bmatrix} y_{r_1} & y_{r_1}^2 & y_{r_1}^{2^2} & \cdots & y_{r_1}^{2^{n-2}} & y_{r_1}^{2^{n-1}} \\ y_{r_2} & y_{r_2}^2 & y_{r_2}^{2^2} & \cdots & y_{r_2}^{2^{n-2}} & y_{r_2}^{2^{n-1}} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ y_{r_n} & y_{r_n}^2 & y_{r_n}^{2^2} & \cdots & y_{r_n}^{2^{n-2}} & y_{r_n}^{2^{n-1}} \end{bmatrix},$$

where $y_{r_1} = \lambda^{r_1}, y_{r_2} = \lambda^{r_2}, \cdots, y_{r_n} = \lambda^{r_n}$. Let

$P_1 = \prod_{j_1 = r_1}^{r_n} y_{j_1}$; $P_2 = \prod_{r_1 \leq j_1 < j_2 \leq r_n} (y_{j_1} + y_{j_2})$; $P_3 = \prod_{r_1 \leq j_1 < j_2 < j_3 \leq r_n} (y_{j_1} + y_{j_2} + y_{j_3})$;

$\cdots$;

$P_n = (y_{r_1} + y_{r_2} + \cdots + y_{r_n})$

Then we have $\det(A'') = \prod_{j=1}^{n} P_j$. From Theorem 1, we can see that C^n is MDS if and only if $\det(A'')$ is non-zero for all $\{r_1, r_2, \cdots, r_n\} \subseteq \{0, 1, 2, \cdots, n-1, n, n+1, \cdots, 2n-1\}$. Maximum degree of any irreducible term in any P_i can be at most $2n-1$. If $deg(M(\lambda)) \geq 2n$, then none of P_i's will be zero and hence $\mathrm{Det}(A'')$ will be non-zero. Thus $C^n$is an MDS matrix if and only if $deg(M(\lambda)) \geq 2n$ when $\lambda_i = \lambda^{2^{i-1}}$ for $i = 1, \cdots, n$. Hence the proof. □

Relationship with [4]: Berger proposed a method to construct recursive MDS matrix using Gabidulin code. The generator matrix described in Section 3.4 of [4] is of the form

$$G = [V^T|\hat{V}^T] = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(2n-1)} \\ 1 & \alpha^4 & \alpha^8 & \cdots & \alpha^{4(2n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{2^{n-1}} & (\alpha^{2^{n-1}})^2 & \cdots & (\alpha^{2^{n-1}})^{2n-1} \end{bmatrix},$$

where $V = vand[\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^{n-1}}]$, $\hat{V} = genvand[\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^{n-1}}; n, n+1, \cdots, 2n-1]$ and $\{1, \alpha, \alpha^2, \cdots, \alpha^{2n-1}\}$ is a polynomial basis of $\mathbb{F}_{2^m}$. By applying elementary row operations on G we can get its systematic form $[I|A]$. In other words, $(V^T)^{-1}G = (V^T)^{-1}[V^T|\hat{V}^T] = [I|A]$. The first column of the matrix $A = (V^T)^{-1}\hat{V}^T$ gives the z_i's of companion matrix $C = \mathsf{Companion}(z_0, z_1, \cdots, z_{n-1})$ so that C^n gives an MDS matrix. It is easy to check that the eigenvalues of C are $\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^{n-1}}$.

In our construction proposed in - II(b), if we take $\lambda \in \mathbb{F}_{2^s}$ to be an element where the degree t of its minimal polynomial satisfies $n \leq \frac{t}{2} \leq \frac{s}{2}$. Then $\lambda_i = \lambda^{2^{i-1}}$ for $i = 1, \cdots, n$, and so λ_is will be distinct and non-zero and the companion matrix formed using these λ_is as eigenvalues will give the same companion matrix as described in Section 3.4 of [4].

4 Conclusion

This paper gives a general construction of recursive MDS matrix using a companion matrix which is diagonable. Although diagonable property is not required, in general, to construct recursive MDS matrix, it may provide a wide range of companion matrices whose k^{th} power yield MDS matrices. To the best of our knowledge, only two methods are known so far to construct recursive MDS matrix directly using - (a) shortened MDS BCH code and (b) Gabidulin code. We have shown that these two constructions directly come from our proposed constructions - I and IIa) (subsection 2 and 4). We provided one more construction that is related to Gabadulin code.

The necessary and sufficient condition for constructing recursive MDS matrix from non-singular diagonable companion matrix may provide many more constructions to construct recursive MDS matrix from companion matrix. We have given three constructions and the possibilities are many more. And, in future, it could be worth exploring the other possibilities of recursive MDS matrix from non-singular and non-diagonable companion matrix.

References

1. Augot, D. and Finiasz, M.: Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. In *Proceedings of the 2013*

IEEE International Symposium on Information Theory, pages 1551-1555, IEEE, 2013.
2. Augot, D. and Finiasz, M.: Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes. In *Fast Software Encryption, FSE 2014*, LNCS, Springer, 2014, to appear.
3. Augot, D. and Finiasz, M.: Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes. http://eprint.iacr.org/2014/566.pdf
4. Berger, T.P.: Construction of Recursive MDS Diffusion Layers from Gabidulin Codes. In *INDOCRYPT 2013*, Lecture Notes in Computer Science, volume 8250, pages 274-285, Springer, 2013.
5. Berger, T.P. and Ourivski, A.: Construction of new MDS codes from Gabidulin codes. In *Proceedings of ACCT 2009*, Kranevo, Bulgaria, pages 40-47, June, 2004.
6. Barreto, P. and Rijmen, V.: The Khazad Legacy-Level Block Cipher. In *Submission to the NESSIE Project*, 2000, http://cryptonessie.org
7. Daemen, J.: Cipher and hash function design, strategies based on linear and differential cryptanalysis. PhD Thesis. K.U.Leuven, 1995.
8. Daemen, J., Knudsen, L.R. and Rijmen, V.: The block cipher SQUARE. In *Fast Software Encryption 1997*, Lecture Notes in Computer Science, volume 1267, pages 149-165, Springer, 1997.
9. Daemen, J. and Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. In *Information Security and Cryptography*, Springer 2002.
10. Filho, G.D., Barreto, P. and Rijmen, V.: The Maelstrom-0 Hash Function. In *Proceedings of the 6th Brazilian Symposium on Information and Computer Systems Security*, 2006.
11. Gabidulin, E.M.: Theory of codes with maximum rank distance. In *Problems of Information Transmission (English translation of Problemy Peredachi Informatsii)*, 21(1), 1985.
12. Gauravaram, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., Rechberger, C., Schlaffer, M. and Thomsen, S.: Grϕstl a SHA-3 Candidate. In *Submission to NIST*, 2008, http://www.groestl.info
13. Guo, J., Peyrin, T. and Poshmann, A.: The PHOTON Family of Lightweight Hash Functions. In *CRYPTO 2011*, Lecture Notes in Computer Science, volume 6841, pages 222-239, Springer, 2011.
14. Guo, J., Peyrin, T., Poshmann, A. and Robshaw, M.J.B.: The LED block cipher. In *CHES 2011*, Lecture Notes in Computer Science, volume 6917, pages 326-341, Springer, 2011.
15. Gupta, K.C. and Ray, I.G.: On constructions of MDS matrices from companion matrices for lightweight cryptography. In *CD-ARES Workshops 2013*, Lecture Notes in Computer Science, pages 29-43, Springer, 2013.
16. Junod, P. and Vaudenay, S.: Perfect diffusion primitives for block ciphers. In *Selected Areas in Cryptography 2004*, Lecture Notes in Computer Science, volume 3357, pages 84-99, Springer, 2004.
17. Junod, P. and Vaudenay, S.: FOX: A new family of block ciphers. In *Selected Areas in Cryptography 2004*, Lecture Notes in Computer Science, volume 3357, pages 114-129, Springer, 2004.
18. MacWilliams, F.J. and Sloane, N.J.A.: The Theory of Error-Correcting Codes. In *North Holland Publishing Co.*, 1988.
19. Marchi, S.De: Polynomials Arising in Factoring Generalized Vandermonde Determinants: An Algorithm for Computing Their Coefficients. In *Mathematical and Computer Modelling*, Volume 34, Issue 3-4, pages 271-281, Elsevier, August 2001.

20. Nakahara Jr., J. and Abrahao, E.: A New Involutory MDS Matrix for the AES. In *International Journal of Network Security*, 9(2), 109-116, 2009.
21. Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A. and Win, E.D.: The cipher SHARK. In *Fast Software Encryption 1996*, Lecture Notes in Computer Science, pages 99-112, Springer, 1996.
22. Sajadieh, M., Dakhilalian, M., Mala, H. and Sepehrdad, P.: Recursive diffusion layers for block ciphers and hash functions. In *Fast Software Encryption 2012*, Lecture Notes in Computer Science, volume 7549, pages 385-401, Springer, 2012.
23. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. and Ferguson, N.: Twofish: A 128-bit block cipher. In *The first AES Candidate Conference. National Institute for Standards and Technology*, 1998.
24. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. and Ferguson, N.: The Twofish encryption algorithm. Wiley, 1999.
25. Schnorr, C.P. and Vaudenay, S.: Black Box Cryptanalysis of Hash Networks Based on Multipermutations. In *EUROCRYPT 1994*, Lecture Notes in Computer Science, volume 950, pages 47-57, Springer, 1995.
26. Shannon, C.E.: Communication Theory of Secrecy Systems. In *Bell Syst. Technical J.* 28, pages 656-715, 1949.
27. Sony Corporation: The 128-bit Block cipher CLEFIA Algorithm Specification. 2007, http://www.sony.co.jp/Products/cryptography/clefia/download/data/clefia-spec-1.0.pdf
28. Vaudenay, S.: On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER. In *Fast Software Encryption 1994*, Lecture Notes in Computer Science, volume 1008, pages 286-297, Springer, 1995.
29. Watanabe, D., Furuya, S., Yoshida, H., Takaragi, K. and Preneel, B.: A new keystream generator MUGI. In *Fast Software Encryption 2002*, Lecture Notes in Computer Science, volume 2365, pages 179-194, Springer, 2002.
30. Wu, S., Wang, M. and Wu, W.: Recursive diffusion layers for (lightweight) block ciphers and hash functions. In *Selected Areas in Cryptography 2013*, Lecture Notes in Computer Science, volume 7707, pages 355-371, Springer, 2013.