On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography

Kishan Chand Gupta and Indranil Ghosh Ray

Applied Statistics Unit, Indian Statistical Institute.
203, B. T. Road, Kolkata 700108, INDIA.
kishan@isical.ac.in, indranil_r@isical.ac.in

Abstract. Maximum distance separable (MDS) matrices have applications not only in coding theory but also are of great importance in the design of block ciphers and hash functions. It is highly nontrivial to find MDS matrices which could be used in lightweight cryptography. In a crypto 2011 paper, Guo et. al. proposed a new MDS matrix $Serial(1, 2, 1, 4)^4$ over $\mathbb{F}_{2^8}$. This representation has a compact hardware implementation of the AES MixColumn operation. No general study of MDS properties of this newly introduced construction of the form $Serial(z_0, \ldots, z_{d-1})^d$ over $\mathbb{F}_{2^n}$ for arbitrary d and n is available in the literature. In this paper we study some properties of MDS matrices and provide an insight of why $Serial(z_0, \ldots, z_{d-1})^d$ leads to an MDS matrix. For efficient hardware implementation, we aim to restrict the values of z_i's in $\{1, \alpha, \alpha^2, \alpha+1\}$, such that $Serial(z_0, \ldots, z_{d-1})^d$ is MDS for $d = 4$ and 5, where α is the root of the constructing polynomial of $\mathbb{F}_{2^n}$. We also propose more generic constructions of MDS matrices e.g. we construct lightweight 4×4 and 5×5 MDS matrices over $\mathbb{F}_{2^n}$ for all $n \geq 4$. An algorithm is presented to check if a given matrix is MDS. The algorithm directly follows from the basic properties of MDS matrix and is easy to implement.

Key words: Diffusion, Companion matrix, MDS matrix, MixColumn operation, minimal polynomial.

1 Introduction

Claude Shannon, in his paper "Communication Theory of Secrecy Systems" [20], defined *confusion* and *diffusion* as two properties, required for the design of block ciphers. In [7–9], Heys and Tavares showed that the replacement of the permutation layer of Substitution Permutation Networks (SPNs) with a diffusive linear transformation improves the avalanche characteristics of the block cipher which increases the cipher's resistance to differential and linear cryptanalysis. Thus the main application of *MDS matrix* in cryptography is in designing block ciphers and hash functions that provide security against differential and linear cryptanalysis. MDS matrices offer diffusion properties and is one of the vital constituents of modern age ciphers like Advanced Encryption Standard (AES) [3], Twofish [18, 19], SHARK [15] and Square [2]. MDS matrices are also used in the design of hash functions. Hash functions like Maelstrom [4], Grϕstl [5] and PHOTON family light weight hash functions [6] use MDS matrices as main part of their diffusion layers.

Nearly all ciphers use predefined MDS matrices for incorporating diffusion property. Although in some ciphers the possibility of random selection of MDS matrices with some constraint is provided [22]. In this context we would like to mention that in papers [6,11,12,16,22], new constructions of MDS matrices are provided. In [6], authors construct lightweight MDS matrices from *companion* matrices by exhaustive search. In [11], authors construct efficient 4×4 and 8×8 matrices to be used in block ciphers. In [12,16], authors constructed involutory MDS matrices using Vandermonde matrices. In [22], authors construct new involutory MDS matrices using properties of Cauchy matrices.

Authors of [6] defined $Serial(z_0, \ldots, z_{d-1})$, which is the companion matrix of $z_0+z_1x+z_2x^2+\ldots+z_{d-1}x^{d-1}+x^d$. Their objective was to find suitable candidates so that $Serial(z_0, \ldots, z_{d-1})^d$ is an MDS matrix. In [6], authors proposed an MDS matrix $Serial(1, 2, 1, 4)^4$ over $\mathbb{F}_{2^8}$ for AES *MixColumn operation* which has compact and improved hardware footprint [6]. It is to be noted that in $Serial(1, 2, 1, 4)$, $z_0 = z_2 = 1$, $z_1 = 2 = \alpha$ and $z_3 = 4 = \alpha^2$, where α is the root of the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. The proper choice of z_0, z_1, z_2 and z_3 (preferably of low Hamming weight) improves the hardware implementation of AES MixColumn transformation. It may be noted that MixColumn operation in [6] is composed of d ($d = 4$ for AES) applications of the matrix $Serial(z_0, \ldots, z_{d-1})$ to the input column vector. More formally, let $X = (x_0, \ldots, x_{d-1})^T$ be the input column vector of MixColumn and $Y = (y_0, \ldots, y_{d-1})^T$ be the corresponding output. Then we have $Y = A^d \times X = \underbrace{(A \times (A \times (A \times \ldots \times (A}_{\text{d times}} \times X)))) \ldots)$, where $A = Serial(z_0, \ldots, z_{d-1})$. So the hardware circuitry will depend on companion matrix A and not on the MDS matrix A^d. Note that authors of [6] used MAGMA [1] to test all possible values of z_0, z_1, z_2 and z_3 and found $Serial(1, 2, 1, 4)$ to be the right candidate, which raised to the power 4 gives an MDS matrix. Authors of [17,21] proposed new diffusion layers ($d \times d$ MDS matrices) based on companion matrices for smaller values of d. In this paper we provide some sufficient conditions for such constructions but our approach is different from [17,21]. We also propose new and more generic constructions of $d \times d$ MDS matrices for $d = 4$ and 5.

For efficient implementation, we aim to restrict the values of z_i's in the set $\{1, \alpha, \alpha^2, \alpha+1\}$, such that $Serial(z_0, \ldots, z_{d-1})^d$ is MDS, where α is the root of the constructing polynomial of $\mathbb{F}_{2^n}$. It may be noted that multiplication by 1, which is the unit element of $\mathbb{F}_{2^n}$, is trivial. When α is the root of the constructing polynomial of $\mathbb{F}_{2^n}$, the multiplication by α can be implemented by a shift by one bit to the left and a conditional XOR with a constant when a carry bit is set (multiplication by α is often denoted as xtime). Multiplication by $\alpha + 1$ is done by a multiplication by α and one XOR operation. Multiplication by α^2 is done by two successive multiplication by α. We also explore some properties of MDS matrices and based on that we provide an algorithm to check whether the matrix is MDS. This algorithm is easy to implement. We implement the algorithm and run it for upto 8×8 matrices over $\mathbb{F}_{2^{24}}$.

In general we also study the cases where we restrict the values of z_i's in the set $\{1, \beta, \beta^2, \beta+1\}$ for any non zero $\beta \in \mathbb{F}_{2^n}$, such that $Serial(z_0, \ldots, z_{d-1})^d$ is MDS.

The paper is organized as follows: In Section 2 we provide definitions and preliminaries. In Section 3, we discuss a few relevant properties of MDS matrices. In Section 4 and Subsections therein, we study $Serial(z_0, z_1, z_2, z_3)^4$ and $Serial(z_0, z_1, z_2, z_3, z_4)^5$ and propose new constructions of MDS matrices. At the end of Section 4, we present an algorithm to check if a given square matrix is MDS. We conclude the paper in Section 5.

2 Definition and Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field with two elements and $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. We will often denote a matrix by $((a_{i,j}))$, where $a_{i,j}$ is the (i, j)-th element of the matrix. The *Hamming weight* of an integer i is the number of non zero coefficients in the binary representation of i and is denoted by $\mathrm{H}(i)$. For example $\mathrm{H}(5) = 2$, $\mathrm{H}(8) = 1$.

A *cyclotomic coset* C_s modulo $(2^n - 1)$ is defined as [13, page 104]

$$C_s = \{s, s \cdot 2, \cdots, s \cdot 2^{n_s - 1}\}$$

where n_s is the smallest positive integer such that $s \equiv s2^{n_s} (\mathrm{mod}\ 2^n - 1)$. The subscript s is the smallest integer in C_s, and is called the *coset leader* of C_s. Note that n_s is the size of the coset C_s which will also be denoted by $|C_s|$. When $n_s = n$, we call it a full length coset and when $n_s < n$, we call it a smaller coset. The set of all coset leaders modulo $(2^n - 1)$ is denoted by $\Upsilon(n)$. The computations in cosets are performed in $\mathbb{Z}_{2^n-1}$, the ring of integers modulo $(2^n - 1)$. For $n = 4$ the cyclotomic cosets modulo $2^4 - 1 = 15$ are: $C_0 = \{0\}, C_1 = \{1, 2, 4, 8\}, C_3 = \{3, 6, 12, 9\}, C_5 = \{5, 10\}, C_7 = \{7, 14, 13, 11\}$. Note $|C_5| = 2$, $|C_1| = 4$, and $\Upsilon(4) = \{0, 1, 3, 5, 7\}$.

Let $\beta \in \mathbb{F}_{p^n}$, p being a prime number. The *minimal polynomial* [13, page 99] over $\mathbb{F}_p$ of β is the lowest degree monic polynomial, say $M(x)$, with coefficients from $\mathbb{F}_p$ such that $M(\beta) = 0$. It is easy to check that the minimal polynomial is irreducible [13, page 99]. If $f(x)$ is any polynomial over $\mathbb{F}_p$ such that $f(\beta) = 0$, then $M(x)|f(x)$ [13, page 99].

Using the notation of [6], we define $Serial(z_0, \ldots, z_{d-1})$ as follows.

$$Serial(z_0, \ldots, z_{d-1}) = \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ z_0 & z_1 & \ldots & \ldots & \ldots & z_{d-1} \end{pmatrix},$$

where $z_0, z_1, z_2, \ldots, z_{d-1} \in \mathbb{F}_{2^n}$ for some n. Note that this matrix is a companion matrix of the polynomial $z_0 + z_1 x + z_2 x^2 + \ldots + z_{d-1} x^{d-1} + x^d$.

We note that,

$$Serial(z_0, \ldots, z_{d-1})^{-1} = \begin{pmatrix} \frac{z_1}{z_0} & \frac{z_2}{z_0} & \ldots & \ldots & \ldots & \frac{1}{z_0} \\ 1 & 0 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}. \quad (1)$$

It is to be noted that like encryption, decryption can also be implemented by repeated use (d times) of $Serial(z_0, \ldots, z_{d-1})^{-1}$, and also whenever $z_0 = 1$, the hardware footprint for decryption is as good as that of encryption circuitry.

Definition 1. *Let $\mathbb{F}$ be a finite field and p and q be two integers. Let $x \to M \times x$ be a mapping from $\mathbb{F}^p$ to $\mathbb{F}^q$ defined by the $q \times p$ matrix M. We say that it is an MDS matrix if the set of all pairs $(x, M \times x)$ is an MDS code, i.e. a linear code of dimension p, length $p + q$ and minimal distance $q + 1$.*

An MDS matrix provides diffusion properties that have useful applications in cryptography. The idea comes from coding theory, in particular from maximum distance separable codes (MDS codes). In this context we state two important theorems of Coding Theory.

Theorem 1. *[13, page 33] If C is an $[n, k, d]$ code, then $n - k \geq d - 1$.*

Codes with $n - k = d - 1$ are called maximum distance separable codes, or MDS codes for short.

Theorem 2. *[13, page 321] An $[n, k, d]$ code C with generator matrix $G = [I|A]$, where A is a $k \times (n - k)$ matrix, is MDS if and only if every square submatrix (formed from any i rows and any i columns, for any $i = 1, 2, \ldots, min\{k, n - k\}$) of A is nonsingular.*

The following fact is another way to characterize an MDS matrix.

Fact: 1 *A square matrix A is an MDS matrix if and only if every square submatrices of A are nonsingular.*

Fact: 2 *All entries of an MDS matrix are non zero.*

3 Few Properties Of MDS Matrices

In this Section we develop some tools for studying $Serial(z_0, z_1, z_2, z_3)^4$, $z_i \in \mathbb{F}_{2^n}$. We also use these tools to provide an algorithm to check whether a matrix is MDS.

It may be noted that from the entries of the inverse of a $d \times d$ nonsingular matrix, it can be checked whether all its $(d-1) \times (d-1)$ submatrics are nonsingular or not. In this direction we state the following Lemma which will be used in Algorithm 1.

Lemma 1. *All entries of inverse of MDS matrix are non zero.*

Proof. Let $\mathbb{M} = ((m_{i,j}))$ be a $d \times d$ MDS matrix. We know that $M^{-1} = Adj(\mathbb{M})^t / det(\mathbb{M})$, where $Adj(\mathbb{M}) = ((M_{i,j}))$ and $M_{i,j}$ is co-factor of $m_{i,j}$ in $\mathbb{M}$ which is the determinant of $(d-1) \times (d-1)$ submatrix obtained by omitting i'th row and j'th column of $\mathbb{M}$. Since $\mathbb{M}$ is an MDS matrix, all its $(d - 1) \times (d - 1)$ submatrices are nonsingular. Thus all $M_{i,j}$ values are non zero. □

Corollary 1. *Any 2×2 matrix over $\mathbb{F}_{2^n}$ is MDS matrix if and only if it is a full rank matrix and all entries of its inverse is non zero.*

Proof. Let $((a_{i,j}))$ be a 2×2 full rank matrix and let all entries of its inverse be non zero. Let its inverse matrix be $((b_{i,j}))$. It is easy to check that $b_{0,0} = a_{0,0}$, $b_{1,1} = a_{1,1}$, $b_{0,1} = -a_{1,0}$ and $b_{1,0} = -a_{0,1}$. Thus all entries of $((a_{i,j}))$ are non zero. So all square submatrices of $((a_{i,j}))$ are nonsingular. So $((a_{i,j}))$ is MDS.

The other direction of the proof is immediate. □

Corollary 2. *Any 3×3 matrix over $\mathbb{F}_{2^n}$ with all non zero entries is an MDS matrix if and only if it is a full rank matrix and all entries of its inverse are non zero.*

Proof. Let $\mathbb{M} = ((m_{i,j}))$ be a 3×3 full rank matrix with all non zero entries, such that its inverse matrix also has got all non zero entries. So, all 2×2 submatrices of $\mathbb{M}$ are nonsingular. Note that all 1×1 submatrices, which are nothing but the elements $m_{i,j}$'s, are also non zero. Thus the matrix is MDS matrix.

The other direction of the proof is immediate. □

Lemma 2. *It may be noted that if all the entries of the inverse of a $d \times d$ nonsingular matrix are non zero, then all its $(d-1) \times (d-1)$ submatrics are nonsingular.*

In the next Proposition we study the necessary and sufficient condition for any 4×4 matrix to be MDS. This Proposition will be referred to at many places throughout the paper.

Proposition 1. *Any 4×4 matrix over $\mathbb{F}_{2^n}$ with all entries non zero is an MDS matrix if and only if it is a full rank matrix with the inverse matrix having all entries non zero and all of its 2×2 submatrices are full rank.*

Proof. Let $\mathbb{M} = ((m_{i,j}))$ be a 4×4 matrix satisfying the conditions of this proposition. Since its inverse matrix has all non zero entries, therefore by Fact 2, all $(4-1) \times (4-1)$ i.e. 3×3 submatrices of $\mathbb{M}$ are full rank matrices. Also inverse matrices of all 2×2 submatrices are full rank. Therefor all square submatrices of $((m_{i,j}))$ are full rank. Thus the matrix is MDS. The other direction of the proof is immediate. □

4 MDS Properties of $Serial(z_0, z_1, z_2, z_3)^4$

In this Section we consider low Hamming weight candidates $z_0, z_1, z_2, z_3 \in \mathbb{F}_{2^n}$ for arbitrary n, such that $Serial(z_0, z_1, z_2, z_3)^4$ is MDS. Low Hamming weight coefficients are desirable for better hardware implementation. So we restrict the values of z_i's to 1, α, α^2, $1 + \alpha$, and also try to maximize the occurrence of 1', where α is the root of constructing polynomial of $\mathbb{F}_{2^n}$. At the end of this Section we present an algorithm to check if a given $d \times d$ matrix is MDS.

Now we provide cases (from Lemma 3 to Lemma 9) for which $Serial(z_0, z_1, z_2, z_3)^4$ is non MDS except for one special case of Lemma 8 (see Remark 3). In Subsection 4.1 and Subsection

4.2, we will construct lightweight 4×4 MDS matrices and in Subsection 4.3 we will construct lightweight 5×5 MDS matrices of the form $Serial(z_0, z_1, z_2, z_3, z_4)^5$.

Lemma 3. *$Serial(1,1,1,1)^4$ is not an MDS matrix.*

Proof. It is easy to check that,

$$Serial(1,1,1,1)^4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

From Theorem 2, we know that all square submatrices of an MDS matrix are nonsingular. So all entries of an MDS matrix must be non zero. So clearly $Serial(1,1,1,1)^4$ is not an MDS matrix. □

When 1 is placed in three out of four positions z_0, z_1, z_2 and z_3, four such matrices can be formed all of which are non MDS. Towards this we have the next lemma.

Lemma 4. *$Serial(z_0, z_1, z_2, z_3)^4$ is never an MDS matrix when any three of $\{z_0, z_1, z_2, z_3\}$ are 1.*

Proof. The proof techniques are similar to the proof of Lemma 3. □

Remark 1. We try to restrict values of z_i's to $1, \alpha, \alpha^2, \alpha+1$ and try to maximize the occurrence of 1's in the matrix $Serial(z_0, z_1, z_2, z_3)$ for better hardware implementation. If 1 is allowed in all four places $z_0, z_1, z_2,$ and z_3, the matrix $Serial(z_0, z_1, z_2, z_3)^4$ is not MDS (from Lemma 3). Similarly, from Lemma 4, $Serial(z_0, z_1, z_2, z_3)^4$ is non MDS, where any three out of $z_0, z_1, z_2,$ and z_3 are 1. We next study the possibility of having MDS matrices of the form $Serial(z_1, z_2, z_3, z_4)^4$ when any two out of $z_0, z_1, z_2,$ and z_3 are 1. Note that there are 6 such cases. It is easy to check that out these 6 cases, $Serial(z_0, z_1, 1, 1)^4$ and $Serial(z_0, 1, z_2, 1)^4$ will never be MDS. Also $Serial(1, 1, z_2, z_3)^4$ and $Serial(1, z_1, z_2, 1)^4$ are non MDS if $z_1, z_2, z_3 \in \{\alpha, \alpha^2, \alpha+1\}$ (see Lemma 5 and Lemma 6). So we concentrate on remaining two cases, i.e. $Serial(1, z_1, 1, z_3)^4$ and $Serial(z_0, 1, 1, z_3)^4$.

While studying $Serial(z_0, z_1, z_2, z_3)^4$, we fix two of z_0, z_1, z_2, z_3 at 1 and restrict the other two entries to $\alpha, \alpha^2, \alpha+1$. Note that when these two values are distinct, they can be from one of the sets $\{\alpha, \alpha^2\}$, $\{\alpha, \alpha+1\}$ and $\{\alpha+1, \alpha^2\}$. In Section 4 we will form MDS matrices from the first two sets for efficient implementations. Towards this we provide the following lemmas without proof.

Lemma 5. *Let $S = Serial(1, 1, z_2, z_3)$ and $z_2, z_3 \in \{\alpha, \alpha^2, \alpha+1\}$, which are defined over $\mathbb{F}_{2^n}$, where α is the root of constructing polynomial of $\mathbb{F}_{2^n}$. Then S^4 is non MDS matrix.*

Lemma 6. *Let $S = Serial(1, z_1, z_2, 1)$, which is defined over $\mathbb{F}_{2^n}$, where α is the root of constructing polynomial of $\mathbb{F}_{2^n}$ and $z_1, z_2 \in \{\alpha, \alpha^2, \alpha+1\}$. Then S^4 is non MDS matrix.*

Since we are looking for low Hamming weight matrices, we concentrate on remaining two cases of Remark 1, i.e. $Serial(1, z_1, 1, z_3)^4$ and $Serial(z_0, 1, 1, z_3)^4$ for $z_0, z_1, z_3 \in \{\alpha, \alpha^2, \alpha+1\}$.

Lemma 7. *Let $A = Serial(1, \alpha, 1, \alpha^2)$ and $A' = Serial(1, \alpha^2, 1, \alpha)$ which are defined over $\mathbb{F}_{2^n}$, where $1 \leq n \leq 4$ and α is the root of constructing polynomial of $\mathbb{F}_{2^n}$. Then A^4 and A'^4 are non MDS matrix.*

Proof.

$$A^4 = \begin{pmatrix} 1 & \alpha & 1 & \alpha^2 \\ \alpha^2 & \alpha^3+1 & \alpha^2+\alpha & \alpha^4+1 \\ \alpha^4+1 & \alpha^5+\alpha^2+\alpha & \alpha^4+\alpha^3 & \alpha^6+\alpha \\ \alpha^6+\alpha & \alpha^7+\alpha^4+\alpha^2+1 & \alpha^6+\alpha^5+\alpha^2 & \alpha^8+\alpha^4 \end{pmatrix} \tag{2}$$

and

$$A^{-4} = \begin{pmatrix} \alpha^4+\alpha^2 & \alpha^4+\alpha^3+\alpha & \alpha^5+\alpha^4+\alpha^2+1 & \alpha^3+\alpha^2 \\ \alpha^3+\alpha^2 & \alpha^3+\alpha^2 & \alpha^4+\alpha^2+\alpha & \alpha^2+1 \\ \alpha^2+1 & \alpha^2+\alpha & \alpha^3+1 & \alpha \\ \alpha & 1 & \alpha^2 & 1 \end{pmatrix} \tag{3}$$

Note that three irreducible polynomials of degree 4 are x^4+x+1, x^4+x^3+1 and $x^4+x^3+x^2+x+1$. It is easy to observe that $A^4[2][1] = \alpha^5+\alpha^2+\alpha = \alpha(\alpha^4+\alpha+1)$, $A^4[3][2] = \alpha^6+\alpha^5+\alpha^2 = \alpha^2(\alpha^4+\alpha^3+1)$ and $A^4[3][0] = \alpha^6+\alpha = \alpha(\alpha^5+1) = \alpha(\alpha+1)(\alpha^4+\alpha^3+\alpha^2+\alpha+1)$. So, when the minimal polynomial of α is x^4+x+1 or x^4+x^3+1 or $x^4+x^3+x^2+x+1$, $A^4[2][1]$ or $A^4[3][2]$ or $A^4[3][0]$ will be 0 respectively. Thus A^4 is a non MDS matrix for $n = 4$.

Similarly, $A^{-4}[0][1] = \alpha^4+\alpha^3+\alpha = \alpha(\alpha^3+\alpha^2+1)$ and $A^{-4}[1][2] = \alpha^4+\alpha^2+\alpha = \alpha(\alpha^3+\alpha+1)$. So, when the minimal polynomial of α is x^3+x^2+1 or x^3+x+1, $A^{-4}[0][1]$ or $A^4[1][2]$ will be zero respectively. Thus A^4 is a non MDS matrix for $n = 3$.

Again $A^4[1][1] = \alpha^3+1 = \alpha(\alpha^2+\alpha+1)$ which is zero when the minimal polynomial of α is x^2+x+1. Thus A^4 is a non MDS matrix for $n = 2$.

Lastly, when $n = 1$, α is 1, making $A = Serial(1, 1, 1, 1)$ and from Lemma 3, A^4 will be a non MDS matrix.

Similarly it can be proved that A'^4 is non MDS matrix. □

Remark 2. $Serial(1, \alpha, 1, \alpha+1)^4$, defined over $\mathbb{F}_{2^n}$, is non MDS for $1 \leq n \leq 3$. The proof is similar to Lemma 7. In Section 4, Proposition 3, we will show that $Serial(1, \alpha, 1, \alpha+1)^4$ is MDS for all $n \geq 4$.

Lemma 8. *Let $B = Serial(\alpha, 1, 1, \alpha^2)$ and $B' = Serial(\alpha^2, 1, 1, \alpha)$ which are defined over $\mathbb{F}_{2^n}$, where $1 \leq n \leq 4$ and α is the root of the constructing polynomial of $\mathbb{F}_{2^n}$. Then B^4 is non MDS matrix except when $n = 4$ and α is a root of x^4+x+1. Also B'^4 is non MDS for all n such that $1 \leq n \leq 4$.*

Proof.

$$B^4 = \begin{pmatrix} \alpha & 1 & 1 & \alpha^2 \\ \alpha^3 & \alpha^2+\alpha & \alpha^2+1 & \alpha^4+1 \\ \alpha^5+\alpha & \alpha^4+\alpha^3+1 & \alpha^4+\alpha^2+\alpha+1 & \alpha^6+1 \\ \alpha^7+\alpha & \alpha^6+\alpha^5+\alpha+1 & \alpha^6+\alpha^4+\alpha^3 & \alpha^8+\alpha^4+\alpha+1 \end{pmatrix} \tag{4}$$

also

$$B^{-4} = \frac{1}{\alpha}\begin{pmatrix} \alpha^3+\alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 & \alpha^6+\alpha & \alpha^4+1 \\ \alpha^5+\alpha & \alpha^4+\alpha^3+\alpha^2+\alpha & \alpha^4+\alpha^3+\alpha^2 & \alpha^2+\alpha \\ \alpha^3+\alpha^2 & \alpha^5+\alpha^2 & \alpha^4+\alpha^3 & \alpha^2 \\ \alpha^3 & \alpha^3 & \alpha^5 & \alpha^3 \end{pmatrix} \tag{5}$$

The list of determinants of all 36, 2×2 submatrices of B^4 are $1,\ \alpha,\ 1,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^3+1,\ \alpha^2,\ \alpha^3+1,\ \alpha^2+\alpha,\ \alpha^4+\alpha^2+\alpha,\ \alpha^4+\alpha^3+\alpha^2,\ \alpha^5+\alpha,\ \alpha^4+1,\ \alpha^5+\alpha^2+\alpha,\ \alpha^4+\alpha^3,\ \alpha^6+\alpha^4+\alpha^3+\alpha^2+1,\ \alpha^6+\alpha^5+\alpha^4+\alpha^2,\ \alpha^7,\ 1,\ \alpha^2+\alpha,\ \alpha^3+1,\ \alpha^3+\alpha^2,\ \alpha^4+\alpha^2,\ \alpha^4+\alpha^2,\ \alpha^2+\alpha,\ \alpha^4+\alpha^3+\alpha^2,\ \alpha^5+\alpha,\ \alpha^5+\alpha^4+\alpha^3+\alpha,\ \alpha^6+\alpha^4+\alpha^2+1,\ \alpha^6+\alpha^2,\ \alpha^3+1,\ \alpha^4+\alpha^2,\ \alpha^4+\alpha^2,\ \alpha^5,\ \alpha^3+\alpha,\ \alpha^6+\alpha^3$.

There are three irreducible polynomials with coefficients from $\mathbb{F}_2$ and degree 4, namely x^4+x+1, x^4+x^3+1 and $x^4+x^3+x^2+x+1$. It is easy to observe that $B^4[2][1] = \alpha^4+\alpha^3+1$ and $B^4[3][1] = \alpha^6+\alpha^5+\alpha+1 = (\alpha+1)^2(\alpha^4+\alpha^3+\alpha^2+\alpha+1)$. Thus, when the minimal polynomial of α is x^4+x^3+1 or $x^4+x^3+x^2+x+1$, $B^4[2][1]$ or $B^4[3][1]$ will be 0 respectively. Also note that no polynomial in the above list or in the entries of B^4 or its inverse is a multiple of $\alpha^4+\alpha+1$. Thus B^4 is a non MDS matrix for $n=4$ when the minimal polynomial of α is x^4+x+1.

It is easy to observe that $B^4[3][2] = \alpha^6+\alpha^4+\alpha^3 = \alpha^3(\alpha^3+\alpha+1)$ and $B^4[2][2] = \alpha^4+\alpha^2+\alpha+1 = (\alpha+1)(\alpha^3+\alpha^2+1)$. So, when the minimal polynomial of α is x^3+x+1 or x^3+x^2+1, $B^4[3][2]$ or $B^4[2][2]$ will be zero respectively. Thus B^4 is non a MDS matrix for $n=3$.

Again $B^4[2][3] = \alpha^6+1 = (\alpha+1)^2(\alpha^2+\alpha+1)^2$ which is zero when the minimal polynomial of α is x^2+x+1. Thus B^4 is non a MDS matrix for $n=2$.

Lastly, when $n=1$, α is 1, making $B = Serial(1,1,1,1)$ and from Lemma 3, B^4 will be non MDS matrix.

Similarly it can be proved that B'^4 is non MDS matrix. □

Remark 3. Note for $n=4$, if the Galois field $\mathbb{F}_{2^4}$ is constructed by x^4+x+1 then we can construct an MDS matrix $Serial(\alpha,1,1,\alpha^2)^4$ where α is the root of x^4+x+1.

Lemma 9. *Let $A = Serial(\alpha,1,1,\alpha+1)$ and $A' = Serial(\alpha+1,1,1,\alpha)$ which are defined over $\mathbb{F}_{2^n}$, where α is the root of the constructing polynomial of $\mathbb{F}_{2^n}$. Then A^4 and A'^4 are non MDS matrices.*

Proof. The proof technique is similar to that used in the proof of 7. □

So far we have mainly considered the cases for which the constructed matrices are non MDS. Now we consider the cases for which the matrices are MDS.

4.1 Lightweight MDS matrix of the form $Serial(1, z_1, 1, z_3)^4$

In this Subsection, we study the MDS property of the matrices of the form $Serial(1, z_1, 1, z_3)^4$. We concentrate on $z_1, z_3 \in \{\alpha, \alpha^2, \alpha + 1\}$ for better hardware implementation, where α is the root of constructing polynomial of $\mathbb{F}_{2^n}$ for different n. Here $z_0 = 1$. $Serial(1, z_1, 1, z_3)^{-1}$ is as defined in equation 1 with $d = 4$. So the hardware footprint for decryption is as good as that of encryption circuit in Substitution Permutation Networks (SPNs).

Proposition 2. *Let $A = Serial(1, \alpha, 1, \alpha^2)$ be a 4×4 matrix over the finite field $\mathbb{F}_{2^n}$ and α is the root of the constructing polynomial of $\mathbb{F}_{2^n}$. Then, A^4 is MDS for all $n \geq 5$ except when $n = 6$ and α is root of $x^6 + x^5 + x^4 + x + 1 = 0$.*

Proof. The minimal polynomial of α must be of degree $n \geq 5$. From equation 2 and 3, we get A^4 and A^{-4}. It is easy to check that $A^4[2][1] = \alpha^5+\alpha^2+\alpha = \alpha(\alpha^4+\alpha+1) \neq 0$, $A^4[2][3] = A^4[3][0] = \alpha^6 + \alpha = \alpha(\alpha + 1)(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) \neq 0$, $A^4[3][2] = \alpha^6 + \alpha^5 + \alpha^2 = \alpha^2(\alpha^4 + \alpha^3 + 1) \neq 0$, $A^4[3][3] = \alpha^8 + \alpha^4 = \alpha^4(\alpha + 1)^4 \neq 0$, $A^{-4}[0][2] = \alpha^5 + \alpha^4 + \alpha^2 + 1 = (\alpha + 1)(\alpha^4 + \alpha + 1) \neq 0$.

Out of all polynomials in α that are occurring in the entries of A^4 and its inverse, the above polynomials are of degree more than 5 and rest of the entries are of degree less than 5 except $A^4[3][2] = \alpha^7 + \alpha^4 + \alpha^2 + 1 = (\alpha + 1)(\alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1)$. So $A^4[3][2] = 0$ if $n = 6$ and α is the root of $x^6 + x^5 + x^4 + x + 1 = 0$. Thus all entries of A^4 and its inverse are non zero for $n \geq 5$ except when $n = 6$ and α is root of $x^6 + x^5 + x^4 + x + 1 = 0$.

It is easy to check that the number of 2×2 submatrices of A^4 is 36. Determinants of all these 2×2 submatrices of A^4 are

$1,\ \alpha,\ 1,\ \alpha^2 + 1,\ \alpha^2 + \alpha,\ \alpha^3 + 1,\ \alpha^2,\ \alpha^3 + 1,\ \alpha^2 + \alpha,\ \alpha^4 + \alpha^2 + \alpha,\ \alpha^4 + \alpha^3 + \alpha^2,\ \alpha^5 + \alpha,\ \alpha^4 + 1,\ \alpha^5 + \alpha^2 + \alpha,\ \alpha^4 + \alpha^3,\ \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1,\ \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2,\ \alpha^7,\ 1,\ \alpha^2 + \alpha,\ \alpha^3 + 1,\ \alpha^3 + \alpha^2,\ \alpha^4 + \alpha^2,\ \alpha^4 + \alpha^2,\ \alpha^2 + \alpha,\ \alpha^4 + \alpha^3 + \alpha^2,\ \alpha^5 + \alpha,\ \alpha^5 + \alpha^4 + \alpha^3 + \alpha,\ \alpha^6 + \alpha^4 + \alpha^2 + 1,\ \alpha^6 + \alpha^2,\ \alpha^3 + 1,\ \alpha^4 + \alpha^2,\ \alpha^4 + \alpha^2,\ \alpha^5,\ \alpha^3 + \alpha,\ \alpha^6 + \alpha^3$.

Note that all 36 polynomials are of degree < 8. Thus all these 36 polynomials in α are non zero.

It is evident that these polynomials in this list which are of degree less than 5 are non zero. Rest of the polynomials in the list having degree $\geq n = 5$ are
$\alpha^5 + \alpha, \alpha^5 + \alpha^2 + \alpha, \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1, \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2, \alpha^7, \alpha^5 + \alpha, \alpha^5 + \alpha^4 + \alpha^3 + \alpha, \alpha^6 + \alpha^4 + \alpha^2 + 1, \alpha^6 + \alpha^2, \alpha^5, \alpha^6 + \alpha^3$.
It is easy to check that these values are all non zero as all can be factored into lower degree polynomials of degree less than 5. Thus from Proposition 1, A^4 is an MDS matrix. □

Now we consider $Serial(1, \alpha, 1, \alpha+1)^4$ and provide the following proposition without proof.

Proposition 3. *Let $A = Serial(1, \alpha, 1, \alpha + 1)$ defined over $\mathbb{F}_{2^n}$, where $n \geq 4$ and α is the root of constructing polynomial of $\mathbb{F}_{2^n}$. Then A^4 is MDS matrix.*

Remark 4. It is easy to check that when $n = 8$ and α is the root of irreducible polynomial $x^8+x^4+x^3+x+1$, we get the MDS matrix $Serial(1, \alpha, 1, \alpha^2)^4$, which is proposed in [6]. It may also be noted that by Proposition 3, we get another efficient MDS matrix $Serial(1, \alpha, 1, \alpha+1)^4$.

Now we study $Serial(1, \beta, 1, \beta^2)^4$ for any non zero $\beta \in \mathbb{F}_{2^n}$. So far, we restricted β, to be the root of the constructing polynomial of $\mathbb{F}_{2^n}$. It is easy to note that $\beta = \gamma^i$ for some integer i, where γ is any primitive element in $\mathbb{F}_{2^n}$. In Proposition 4 and Proposition 5, we study the case where i belongs to full length coset and in Proposition 6 and Proposition 7, we study the case when i belongs to smaller coset. These propositions resembles the earlier propositions of this Subsection and proof techniques are also similar.

Proposition 4. *Let $A = Serial(1, \beta, 1, \beta^2)$ be a 4×4 matrix over the finite field $\mathbb{F}_{2^n}$. Also let γ be any primitive element of $\mathbb{F}_{2^n}$ and $\beta = \gamma^i$ such that $i \in C_s$ and $|C_s| = n$. Then if $n \geq 5$ then A^4 is always an MDS matrix except when $n = 6$ and the minimal polynomial of β is $x^6 + x^5 + x^4 + x + 1$.*

Remark 5. It is easy to check that Proposition 2 is a particular case of Proposition 4. Note, in canonical representation of $\mathbb{F}_{2^n}$, MDS matrix construction from Proposition 2 is more efficient.

Proposition 5. *Let $A = Serial(1, \beta, 1, \beta + 1)$ be a 4×4 matrix over the finite field $\mathbb{F}_{2^n}$. Also let γ be any primitive element of $\mathbb{F}_{2^n}$ and $\beta = \gamma^i$ such that $i \in C_s$ and $|C_s| = n$. Then if $n \geq 4$ then A^4 is always an MDS matrix.*

Proposition 6. *Let $A = Serial(1, \beta, 1, \beta^2)$ be a 4×4 matrix over the finite field $\mathbb{F}_{2^n}$. Also let γ be any primitive element of $\mathbb{F}_{2^n}$ and $\beta = \gamma^i$ such that $i \in C_s$, and $|C_s| = m < n$. Then if $m \geq 5$ then A^4 is always an MDS matrix except when $m = 6$ and the minimal polynomial of β is $x^6 + x^5 + x^4 + x + 1$.*

Proposition 7. *Let $A = Serial(1, \beta, 1, \beta + 1)$ be a 4×4 matrix over the finite field $\mathbb{F}_{2^n}$. Also let γ be any primitive element of $\mathbb{F}_{2^n}$ and $\beta = \gamma^i$ such that $i \in C_s$, and $|C_s| = m < n$. Then if $m \geq 4$ then A^4 is always an MDS matrix.*

We observe that if $Serial(1, \beta, 1, \beta^2)^4$ is an MDS matrix, then $Serial(1, \beta, 1, \beta^2)^{-4}$ and $Serial(1, \beta^2, 1, \beta)^4$ are also MDS. We record this in Lemma 10 and Lemma 11

Lemma 10. *If $Serial(1, \beta, 1, \beta^2)^4$ is an MDS matrix for some $\beta \in \mathbb{F}_{2^n}$, then so is the matrix $Serial(1, \beta, 1, \beta^2)^{-4}$.*

Lemma 11. *If $Serial(1, \beta, 1, \beta^2)^4$ is an MDS matrix for some $\beta \in \mathbb{F}_{2^n}$, then so is the matrix $Serial(1, \beta^2, 1, \beta)^4$.*

4.2 Lightweight MDS matrix of the form $Serial(z_0, 1, 1, z_3)^4$

In the Subsection 4.1, we study the MDS property of the matrices of the form given by $Serial(1, z_1, 1, z_3)^4$ for z_i's in $\{\alpha, \alpha^2, \alpha + 1\}$, where α is the root of constructing polynomial of $\mathbb{F}_{2^n}$ for arbitrary n. In this Subsection we study matrices of the form $Serial(z_0, 1, 1, z_3)^4$ over $\mathbb{F}_{2^n}$ for arbitrary n. In different propositions of this Subsection, we propose MDS matrices of the form $Serial(z_0, 1, 1, z_3)^4$ over $\mathbb{F}_{2^n}$ under different conditions imposed on n, where $z_0, z_3 \in \{\alpha, \alpha^2\}$. Note that if $z_0, z_3 \in \{\alpha, \alpha+1\}$, then the matrices will be non MDS (see Lemma 9). In this Subsection we will construct MDS matrices for better hardware footprint by letting $z_0, z_3 \in \{\alpha, \alpha^2\}$ and ignore the case when $z_0, z_3 \in \{\alpha^2, \alpha + 1\}$.

We observe that no MDS matrix exits of the form $Serial(\alpha, 1, 1, \alpha^2)^4$ over $\mathbb{F}_{2^n}$, where $1 \leq n \leq 3$. In the next Proposition we study $Serial(\alpha, 1, 1, \alpha^2)^4$ over $\mathbb{F}_{2^n}$ where $n \geq 4$. Proposition 8 resembles Proposition 2, so we state it without proof.

Proposition 8. *Let $B = Serial(\alpha, 1, 1, \alpha^2)$ be defined over $\mathbb{F}_{2^n}$ where α be the root of the constructing polynomial of $\mathbb{F}_{2^n}$. Then, B^4 is an MDS matrix for all $n \geq 4$ except when $n = 4$ and α is a root of $x^4 + x^3 + x^2 + x + 1 = 0$ or $x^4 + x^3 + 1 = 0$ or when $n = 7$ and α is root of $x^7 + x^6 + x^5 + x^4 + 1 = 0$.*

Now we consider $Serial(\beta, 1, 1, \beta^2)^4$ for any non zero $\beta \in \mathbb{F}_{2^n}$. In Proposition 9 we study the case for full length coset and in Proposition 10 we study the case for smaller coset.

Proposition 9. *Let $B = Serial(\beta, 1, 1, \beta^2)$ be defined over $\mathbb{F}_{2^n}$. Also let γ be the primitive element of $\mathbb{F}_{2^n}$ and $\beta = \gamma^i$ such that $i \in C_s$ and $|C_s| = n$. Then if $n \geq 4$ then B^4 is always an MDS matrix except when $n = 4$ and the minimal polynomial of β is $x^4 + x^3 + x^2 + x + 1$ or $x^4 + x^3 + 1$ and also when $n = 7$ and the minimal polynomial of β is $x^7 + x^6 + x^5 + x^4 + 1$.*

Proposition 10. *Let $B = Serial(\beta, 1, 1, \beta^2)$ be defined over $\mathbb{F}_{2^n}$. Also let γ be the primitive element of $\mathbb{F}_{2^n}$ and $\beta = \gamma^i$ such that $i \in C_s$, and $|C_s| = m < n$. Then if $m \geq 4$ then B^4 is always an MDS matrix except when $m = 4$ and the minimal polynomial of β is $x^4 + x^3 + x^2 + x + 1$ or $x^4 + x^3 + 1$ and also when $m = 7$ and minimal polynomial of β is $x^7 + x^6 + x^5 + x^4 + 1$.*

Remark 6. Note if $Serial(\beta, 1, 1, \beta^2)^4$ is an MDS matrix, then not necessarily $Serial(\beta, 1, 1, \beta^2)^{-4}$ and $Serial(\beta^2, 1, 1, \beta)^4$ are MDS (See Lemma 10 and Lemma 11).

In this Section we found values of $z \in \mathbb{F}_{2^n}$, such that $Serial(1, z, 1, z^2)^4$ and $Serial(1, z^2, 1, z)^4$ are MDS matrices for all $n \geq 5$ and $Serial(z, 1, 1, z^2)^4$ is an MDS matrix for all $n \geq 4$. It may be checked that for $n = 3$ no $Serial(z_0, z_1, z_2, z_3)^4$ is an MDS having two of its entries as one; though for $n = 3$, many such MDS matrices of the form $Serial(z_0, z_1, z_2, z_3)^4$ exist where exactly one of its entries is one. Take for example $Serial(1, \alpha, \alpha^5, \alpha)^4$, where α is the root of $x^3 + x^2 + 1$. For $n = 2$ and 1, no MDS matrix of the form $Serial(z_0, z_1, z_2, z_3)^4$ exists.

4.3 Lightweight 5×5 MDS matrix of the form $Serial(1, z_1, 1, 1, z_4)^5$

In this Subsection we study $Serial(z_0, z_1, z_2, z_3, z_4)^5$, where $z_0, z_1, z_2, z_3, z_4 \in \mathbb{F}_{2^n}$.

As mentioned in Remark 1, we restrict values of z_i's to $1, \alpha, \alpha^2, \alpha + 1$ and try to maximize the occurrence of 1's in the matrix $Serial(z_0, z_1, z_2, z_3, z_4)$ for better hardware implementation. If 1 is allowed in all five places z_0, z_1, z_2, z_3 and z_4, the matrix $Serial(z_0, z_1, z_2, z_3, z_4)^5$ is not MDS (similar to Lemma 3). Also, $Serial(z_0, z_1, z_2, z_3, z_4)^5$ is non MDS, where any four out of z_0, z_1, z_2, z_3 and z_4 are 1 (similar to Lemma 4). We next study the possibility of having MDS matrices of the form $Serial(z_0, z_1, z_2, z_3, z_4)^5$ when any three out of z_0, z_1, z_2, z_3 and z_4 are 1. Note that there are 10 such cases.

We have the following Proposition similar to Proposition 2.

Proposition 11. *Let $A = Serial(1, \alpha, 1, 1, \alpha^2)$ and $A' = Serial(1, \alpha^2, 1, 1, \alpha)$ which are defined over $\mathbb{F}_{2^n}$, where α is the root of the constructing polynomial of $\mathbb{F}_{2^n}$. Then A^5 and A'^5 are MDS for all $n \geq 8$ except when $n = 8$ and α is the root of $x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1 = 0$.*

Proof. The proof techniques are similar to the proof of Proposition 2. □

We close this Section by providing an algorithm to check if a $d \times d$ matrix is MDS. The algorithm directly follows from Lemma 1, Corollary 1 and Corollary 2. We implement the algorithm and run it for up to 8×8 matrices over $\mathbb{F}_{2^{24}}$.

Algorithm 1 Checking if a $d \times d$ matrix $((a_{i,j}))$over $\mathbb{F}_{2^n}$ is an MDS matrix

Input $n > 1$, irreducible polynomial $\pi(x)$ of degree n, the $d \times d$ matrix $((a_{i,j}))$over $\mathbb{F}_{2^n}$.
Output Outputs a boolean variable b_mds which is true if $((a_{i,j}))$ is an MDS matrix, else is false.

1: $b\_mds = true$.
2: Compute inverse of $((a_{i,j}))$ in $((b_{i,j}))$; If inverse does not exist, set $b\_mds = false$ and goto 13;
3: check if all d^2 entries of $((a_{i,j}))$ and $((b_{i,j}))$ are non zero. If not, set $b\_mds = false$;
4: **if** $(d = 3)$: Go to 13;
5: $t \leftarrow d - 2$;
6: **while** $(t > 1$ & $b\_mds = true)$ **do**
7: List all $\binom{d}{t}^2$ submatrices of dimension $t \times t$ in a list $list\_submatrices$;
8: **for** $(e = 0$; $e < \binom{d}{t}^2$; $e = e + 1)$ **do**
9: Find inverse of $list\_submatrices[e]$ in $((inv\_Matrix_{i,j}))$;
10: **if** $(((inv\_Matrix_{i,j}))$ does not exist or any entry of $((inv\_Matrix_{i,j}))$ is zero$)$: $b\_mds = false$;
11: **if** $(b\_mds = false)$: break the loop and go to 13;
12: $t \leftarrow t - 2$;
13: Set b_mds as output;

One approach of checking if a $d \times d$ matrix M is an MDS is to use $[I|M]$ as a generator matrix and check if the code produced is MDS code. Note, if the underlying field is $\mathbb{F}_{2^n}$, the number of code words will be 2^{nd} and finding the minimum weight non zero code word is NP-complete.

For testing if a matrix is MDS, a naive approach may be to check for non singularity of all its square submatrices. The number of computations in this case will be $n^2 \sum_{i=1}^{d} \binom{d}{i}^2 i^3$. It is easy to check that the number of computations of our algorithm is $n^2 \sum_{i=1}^{d/2} \binom{d}{2i}^2 i^3$ for d even and $n^2 \sum_{i=1}^{d/2} \binom{d}{2i+1}^2 (2i+1)^3$ for d odd.

For example, when $n = 8$ and $d = 4$, number of computations by the naive method is $2^6 \times 800$. In the same context, our algorithm takes only $2^6 \times 44$ computations. So the ratio of number of computations required by the naive method with number of computations required by our method is approximately 18. Note that this ratio is independent of n. When $n = 20$ and $d = 8$, number of computations by the naive method is $20^2 \times 988416$ and that by our method is $20^2 \times 61216$, and the ratio is approximately 16.

5 Conclusion

In this paper, we developed techniques to test if a given $d \times d$ matrix over $\mathbb{F}_{2^n}$ is an MDS matrix. We propose a simple algorithm (Algorithm 1) based on some basic properties of MDS matrix. We run the algorithm for up to $n = 24$ and $d = 8$. It might be of interest to explore how further properties related to MDS matrix can be used to develop more efficient algorithm for checking whether a given matrix is MDS.

We developed theories to justify why matrices of the form given by $Serial(z_0, z_1, z_2, z_3)^4$ and $Serial(z_0, z_1, z_2, z_3, z_4)^5$ over $\mathbb{F}_{2^n}$ are MDS for different values n for low Hamming weight choices of values of z_i's, preferably within the set $\{1, \alpha, \alpha^2, \alpha + 1\}$. This leads to new constructions of 4×4 MDS matrices over $\mathbb{F}_{2^n}$ for all $n \geq 4$ and and 5×5 MDS matrices over $\mathbb{F}_{2^n}$ for all $n \geq 8$. We tried to generalize such results for $Serial(z_0, \ldots, z_{d-1})$ so that $Serial(z_0, \ldots, z_{d-1})^d$ is $d \times d$ MDS matrix for $d > 5$. In doing so, we tried to explore the properties of a companion matrix and its corresponding characteristic polynomial. We use the property that eigen values of a matrix A (in our case $A = Serial(z_0, \ldots, z_{d-1})$) are precisely the roots of the characteristic polynomial (in our case it is $z_0 + z_1 x + z_2 x^2 + \ldots + z_{d-1} x^{d-1} + x^d$); Together with the property that if λ is an eigen value of A, then $f(\lambda)$ is the eigen value of $f(A)$ (in our case $f(x) = x^d$) [14]. But with this simple technique, finding sufficient conditions seem difficult for arbitrary d. It may be interesting to carry out more research to construct $d \times d$ MDS matrix $Serial(z_0, \ldots, z_{d-1})^k$ for $k \geq d$.

References

1. W. Bosma, J. Cannon, and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symbolic Comput, 24(3-4):235-265, 1997, Computational algebra and number theory (London, 1993).
2. J. Daemen, L. R. Knudsen, and V. Rijmen, *The block cipher SQUARE*, In 4th Fast Software Encryption Workshop, LNCS 1267, pp. 149–165, Springer-Verlag, 1997.
3. J. Daemen, and V. Rijmen, *The Design of Rijndael*, Springer-Verlag, 2002.
4. G. D. Filho, P. Barreto, and V. Rijmen, *The Maelstrom-0 Hash Function*, In Proceedings of the 6th Brazilian Symposium on Information and Computer Systems Security (2006).

5. P. Gauravaram, L. R Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schlaffer, and S. Thomsen, *Grøstl a SHA-3 Candidate.*, Submission to NIST (2008). Available at http://www.groestl.info.
6. J. Guo, T. Peyrin, and A. Poschmann, *The PHOTON Family of Lightweight Hash Functions*, In CRYPTO, pp. 222–239, Springer, 2011.
7. H. M. Heys, and S. E. Tavares, *The Design of Substitution-Permutation Networks Resistatnt to Differential and Linear Cryptanalysis*, Proceedings of 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia, pp. 148–155, 1994.
8. H. M. Heys, and S. E. Tavares, *The Design of Product Ciphers Resistatnt to Differential and Linear Cryptanalysis*, Journal Of Cryptography, Vol. 9, No. 1, pp. 1-19, 1996
9. H. M. Heys, and S. E. Tavares, *Avalanche Characteristics of Substitution-Permutation Encryption Networks*, IEEE Trans. Comp., Vol. 44, pp. 1131-1139, Sept 1995
10. J. Nakahara Jr, and E. Abrahao, *A New Involutory MDS Matrix for the AES*, International Journal of Network Security, Vol.9, No.2, pp. 109-116, Sept. 2009.
11. P. Junod, and S. Vaudenay, *Perfect Diffusion Primitives for Block Ciphers Building Efficient MDS Matrices*, Selected Areas in Cryptography 2004: Waterloo, Canada, August 9-10,2004. Revisited papers, Lecture Notes in Computer Science. Springer-Verlag.
12. J. Lacan, and J. Fimes, *Systematic MDS erasure codes based on vandermonde matrices*, IEEE Trans. Commun. Lett. 8(9), 570572 (2004) CrossRef
13. F. J. MacWilliams, and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, 1986.
14. A. R. Rao, and P. Bhimasankaram, *Linear Algebra*, Second Edition, Hindustan Book Agency.
15. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. D. Win, *The cipher SHARK*, In 3rd Fast Software Encryption Workshop, LNCS 1039, pp. 99–112, Springer-Verlag, 1996.
16. M. Sajadieh, M. Dakhilalian, H. Mala, and B. Omoomi, *On construction of involutory MDS matrices from Vandermonde Matrices in $GF(2^q)$*, Des. Codes Cryptography, Vol.64, No.3, pp. 287-308, 2012.
17. M. Sajadieh, M. Dakhilalian, H. Mala, and P. Sepehrdad, *Recursive Diffusion Layers for Block Ciphers and Hash Functions*, FSE, pp. 385–401, 2012.
18. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, *Twofish: A 128-bit block cipher*, In the first AES Candidate Conference. National Institute for Standards and Technology, 1998.
19. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, *The Twofish encryption algorithm*, Wiley, 1999.
20. C. E. Shannon, *Communication Theory of Secrecy Systems*. Bell Syst. Technical J., 28, 656–715 (1949).
21. S. Wu, M. Wang, and W. Wu, *Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions.*, SAC 2012, LNCS 7707, pp. 355–371, , Springer-Verlag Berlin Heidelberg, 2013.
22. A. M. Youssef, S. Mister, and S. E. Tavares, *On the Design of Linear Transformations for Substitution Permutation Encryption Networks*, In School of Computer Science, Carleton University, pp. 40–48, 1997.