Exhaustive Search for Various Types of MDS Matrices

Abhishek Kesarwani[1], Santanu Sarkar[1] and Ayineedi Venkateswarlu[2]

[1] Department of Mathematics, Indian Institute of Technology Madras, Chennai - 600036, INDIA
{1907abhi,sarkar.santanu.bir}@gmail.com

[2] Computer Science Unit, Indian Statistical Institute, Chennai Centre, Chennai - 600029, INDIA
venku@isichennai.res.in

Abstract. MDS matrices are used in the design of diffusion layers in many block ciphers and hash functions due to their optimal branch number. But MDS matrices, in general, have costly implementations. So in search for efficiently implementable MDS matrices, there have been many proposals. In particular, circulant, Hadamard, and recursive MDS matrices from companion matrices have been widely studied. In a recent work, recursive MDS matrices from sparse DSI matrices are studied, which are of interest due to their low fixed cost in hardware implementation. In this paper, we present results on the exhaustive search for (recursive) MDS matrices over $GL(4, \mathbb{F}_2)$. Specifically, circulant MDS matrices of order $4, 5, 6, 7, 8$; Hadamard MDS matrices of order $4, 8$; recursive MDS matrices from companion matrices of order 4; recursive MDS matrices from sparse DSI matrices of order $4, 5, 6, 7, 8$ are considered. It is to be noted that the exhaustive search is impractical with a naive approach. We first use some linear algebra tools to restrict the search to a smaller domain and then apply some space-time trade-off techniques to get the solutions. From the set of solutions in the restricted domain, one can easily generate all the solutions in the full domain. From the experimental results, we can see the (non) existence of (involutory) MDS matrices for the choices mentioned above. In particular, over $GL(4, \mathbb{F}_2)$, we provide companion matrices of order 4 that yield involutory MDS matrices, circulant MDS matrices of order 8, and establish the nonexistence of involutory circulant MDS matrices of order $6, 8$, circulant MDS matrices of order 7, sparse DSI matrices of order 4 that yield involutory MDS matrices, and sparse DSI matrices of order $5, 6, 7, 8$ that yield MDS matrices. To the best of our knowledge, these results were not known before. For the choices mentioned above, if such MDS matrices exist, we provide base sets of MDS matrices, from which all the MDS matrices with the least cost (with respect to d-XOR and s-XOR counts) can be obtained. We also take this opportunity to present some results on the search for sparse DSI matrices over finite fields that yield MDS matrices. We establish that there is no sparse DSI matrix S of order 8 over $\mathbb{F}_{2^8}$ such that S^8 is MDS.

Keywords: Diffusion Layer · MDS Matrix · Circulant Matrix · Hadamard Matrix · Recursive MDS Matrix · Companion Matrix · Sparse DSI Matrix · XOR Count

1 Introduction

The Lightweight Cryptography (LWC) project is an initiative launched by the National Institute of Standards and Technology (NIST) which aims to create reliable solutions to the problem of securing data in constrained environments. Solutions to these problems are typically given by building symmetric cryptosystems that have small footprint in hardware and/or low computational complexity. The diffusion layer is one of the key primitives in the design of block ciphers and hash functions, whose major role is to provide

IACR Transactions on Symmetric Cryptology ISSN 2519-173X, Vol. 2019, No. 3, pp. 231–256
DOI:10.13154/tosc.v2019.i3.231-256

an *avalanche effect*, as this ensures a slight change in inputs causes significant changes in outputs. One way to achieve this is to use MDS matrices as they have optimal *branch number* [Dae95]. The term MDS originates from Coding theory, codes for which the *Singleton bound* is met are called *maximal distance separable codes* [MS77]. Over a period of time, several investigations have been made to construct MDS matrices suitable for cryptographic applications. In particular circulant and Hadamard matrices are widely studied [DR02, GR14, SKOP15, LS16a, LW16, PSA+18]. The early implementations of these matrices are round based. Later in 2011, Guo et al. [GPP11] proposed a new recursive (serialized) method of constructing MDS matrices using companion matrices. Liu et al. [LS16a] observed that the implementation of circulant matrices could also be done in a serialized way. Several constructions of recursive MDS matrices have been studied in [GPP11, WWW12, AF13, KPPY14, AF14, GPV17, SSSM17, TTKS18]. In 2018, Toh et al. [TTKS18] proposed a new matrix structure known as *Diagonal-Serial Invertible (DSI)* matrices and its variants *sparse DSI* matrices. The benefit of using a sparse DSI matrix is that its fixed cost is close to half the cost of other matrix types of the same order (see Table 2). The ultimate goal of this line of research is to obtain MDS matrices with low hardware cost.

In many designs of block ciphers, if the diffusion matrix in encryption is M then the diffusion matrix in decryption is M^{-1}. If the MDS matrix is involutory or orthogonal, then the same matrix can be used in both encryption and decryption, and hence the overall hardware cost can be reduced. It is known that there is no involutory circulant MDS matrix over fields of even characteristic (see [GR14, CL19]). But there exist involutory circulant MDS matrices over the general linear group $GL(m, \mathbb{F}_q)$ (see [LW16]). It is also known that there is no companion matrix over fields of even characteristic which yields an involutory MDS matrix (see [GPV19, Theorem 2]). The involutory Hadamard MDS matrices are studied in [SKOP15].

Many of the constructions consider MDS matrices over finite fields. The finite field $\mathbb{F}_q$ with $q = 2^m$ can be interpreted as the m-dimensional vector space $\mathbb{F}_2^m$. With respect to some basis, the multiplication mapping of an element in $\mathbb{F}_{2^m}^*$ can be interpreted as a nonsingular binary matrix in $GL(m, \mathbb{F}_2)$. So the MDS matrices over $\mathbb{F}_{2^m}$ can also be interpreted as MDS matrices over $GL(m, \mathbb{F}_2)$. In search for efficient MDS matrices, as a generalization, block matrices over $GL(m, \mathbb{F}_2)$ are considered. Despite the impressive progress made so far, exhaustive search for MDS matrices over $GL(m, \mathbb{F}_2)$ has remained elusive for some parameter choices of practical importance. There have been many works that employ some ad hoc techniques to search for efficient MDS matrices over $GL(m, \mathbb{F}_2)$. If the exhaustive search is possible then the best MDS matrices that have the least cost/optimal with respect to some efficiency metrics can be identified. With a naive approach, it is difficult to search for MDS matrices exhaustively for some parameter choices. For instance, the size of the search space of 8×8 circulant matrices over $GL(4, \mathbb{F}_2)$ is approximately 2^{112} as $|GL(4, \mathbb{F}_2)| \approx 2^{14}$. So it is of great interest to study different properties of the block matrices over $GL(4, \mathbb{F}_2)$ to reduce the search space. In practice, the concept of equivalence classes of a particular matrix type is used to reduce the search space, as was done in [LS16a] for circulant matrices and in [SKOP15] for Hadamard matrices. In this work, we present a method to exhaustively search for MDS matrices over $GL(m, \mathbb{F}_2)$ in which we use conjugacy classes and restricted conjugacy classes in order to reduce the search space. We also identify the best MDS matrices over $GL(4, \mathbb{F}_2)$ by considering the hardware cost metrics d-XOR count and s-XOR count.

Our contribution:
We first consider four types of MDS matrices over $GL(4, \mathbb{F}_2)$: circulant, Hadamard, recursive MDS matrices from companion and sparse DSI matrices (see Section 2 for definitions). We also present a one-to-one correspondence between circulant MDS matrices and cyclic MDS matrices, and so it is enough to search for circulant MDS matrices. We

use the conjugacy classes and the restricted conjugacy classes discussed in Section 2.2 to restrict the search to a smaller domain. We apply some space-time trade-off techniques to speed up the search/computation. For this purpose, we exploit the nonsingularity of 2×2 submatrices consisting of some component pairs/triplets. We also use look-up table for inverses of the matrices in $GL(4, \mathbb{F}_2)$. From the set of solutions in the restricted domain, one can easily generate all the solutions in the full domain. We have implemented the search for the following parameter choices: circulant matrices of order $4, 5, 6, 7, 8$, Hadamard matrices of order $4, 8$, companion matrices of order 4, sparse DSI matrices of order $4, 5, 6, 7, 8$. The problem of constructing involutory circulant MDS matrices of order $6, 8$ over $GL(m, \mathbb{F}_2), m = 4, 8$ was mentioned in [LW16]. Also the problem of generalizing the sparse DSI matrices over $GL(m, \mathbb{F}_2)$ was mentioned in [TTKS18]. From the experimental results, we have the following observations. To the best of our knowledge, these results were not known before.

1. There is no circulant/cyclic MDS matrix of order 7 over $GL(4, \mathbb{F}_2)$.
2. There exist circulant/cyclic MDS matrices of order 8 over $GL(4, \mathbb{F}_2)$.
3. There is no involutory circulant/cyclic MDS matrix of order $6, 8$ over $GL(4, \mathbb{F}_2)$.
4. There exists a companion matrix L of order 4 over $GL(4, \mathbb{F}_2)$ such that L^4 is an involutory MDS matrix.
5. There is no sparse DSI matrix S of order n over $GL(4, \mathbb{F}_2)$ such that S^n is MDS for $n = 5, 6, 7, 8$.
6. There is no sparse DSI matrix S of order 4 over $GL(4, \mathbb{F}_2)$ such that S^4 is involutory MDS.

In our experimental results, we consider the hardware cost metrics d-XOR count and s-XOR count to identify the best matrices. From our search results, for the parameter choices considered, where MDS matrices were known before, we establish that they are the best with respect to these metrics. We can also see many negative results on the existence of MDS matrices for some parameter choices. In the first case finding a better MDS matrix than the known ones and in the other case finding an MDS matrix is a futile attempt. Now with our results such unsuccessful attempts can be avoided. We are also able to provide MDS matrices in some cases which were not known before. We provide our experimental results at https://www.isichennai.res.in/~venku/MDS/es_mds.html. The base lists of MDS matrices are also available. One can generate all the MDS matrices using our base lists of matrices, and search exhaustively to find the best matrices with respect to some other cost metrics or suitable for a particular platform of implementation.

Note that, in our search for efficient matrices, we try to optimize the cost with respect to the hardware cost metrics d/s-XOR count, by choosing the components of the matrices having low d/s-XOR count. Recently there have been many works which try to optimize the total cost by considering the full matrix instead of local optimization. The first work [KLSW17] in this line exhibits an implementation of AES MixColumn matrix with 97 XOR gates. In [BFI19, TP19] some improved heuristics are proposed to get better implementations of binary matrices in the sense of the number of XOR gates required. As pointed by the anonymous reviewers, it is possible to have implementations with less number of XOR gates when considered the cost of full matrix implementation for the matrices presented in the appendix. In future we would like to apply global optimization tools for the matrices considered. We will make the results available at https://www.isichennai.res.in/~venku/MDS/es_mds.html.

Next we consider sparse DSI matrices over finite fields. In [TTKS18] the authors have provided examples of sparse DSI matrices for some parameter values, and it was mentioned

as an open problem to construct higher order sparse DSI matrices. For this purpose, we first analyze the structure of (sparse) DSI matrices over finite fields. We provide several results on the equivalence of these matrices in the sense of preserving MDS property. By using these results, we are able to search exhaustively for MDS matrices that can be obtained from the sparse DSI matrices of order n over $\mathbb{F}_{2^m}$ for $n = 4, 5, 6, 7, 8$ and $m = 4, 5, 6, 7, 8$, and for $n = 8$ and $m = 9$. Also note that it is possible to search for higher order recursive MDS matrices of this type with our idea. From the experimental results, we have the following observations.

1. There is no sparse DSI matrix S of order 8 over $\mathbb{F}_{2^m}$ for $m = 4, 5, 6, 7, 8$ such that S^8 is MDS.
2. We have a recursive MDS matrix from sparse DSI matrices of order 7 which is better than the known ones.

In the next section we provide notation and definitions. We also provide some basic results that we use later. In Section 2.1 we discuss the hardware cost metrics d-XOR count and s-XOR count. In Section 2.2 we discuss conjugacy classes and restricted conjugacy classes. In Section 3 we first discuss some basic results. We then present our results on reducing the search space for circulant matrices. We discuss this case in more details. Later we present similar search techniques for Hadamard, companion and sparse DSI matrices. In Section 3.5 we consider the case of sparse DSI matrices over finite fields. We provide some experimental results in the appendix. We conclude this paper in Section 4.

2 Notation and Preliminaries

Let $\mathbb{F}_q$ be the finite field containing q elements with $char(\mathbb{F}_q) = 2$. The ring of $m \times m$ matrices over $\mathbb{F}_q$ is denoted by $\mathcal{M}(m, \mathbb{F}_q)$ and the general linear group consisting of nonsingular $m \times m$ matrices over $\mathbb{F}_q$ is denoted by $GL(m, \mathbb{F}_q)$. For simplicity we use $\mathcal{M}_m$ for $\mathcal{M}(m, \mathbb{F}_2)$. We consider some special matrices where the entries are either from the finite field $\mathbb{F}_q$ or from the matrix ring $\mathcal{M}_m$. Let $\mathcal{M}(n, m)$ be the set of $n \times n$ block matrices over $\mathcal{M}_m$ and $\mathcal{D}(n, m)$ be the set of block diagonal matrices over $GL(m, \mathbb{F}_2)$. Also let $\mathcal{P}(n, m)$ be the set of $n \times n$ block permutation matrices over $\mathcal{M}_m$ and $\mathcal{P}_m$ be the set of $m \times m$ permutation matrices over $\mathbb{F}_2$. So the elements of $\mathcal{M}(n, m)$, $\mathcal{D}(n, m)$ and $\mathcal{P}(n, m)$ can be viewed as $mn \times mn$ binary matrices. Note that the matrices in $\mathcal{D}(n, m)$ and $\mathcal{P}(n, m)$ are nonsingular. For $M \in \mathcal{M}(n, m)$, the (i, j)-th entry of the block matrix M is denoted by $M[i, j]$ for $0 \leq i, j \leq n - 1$. We denote a matrix $D \in \mathcal{D}(n, m)$ with $Diag(\mathtt{P}_0, \ldots, \mathtt{P}_{n-1})$, where $\mathtt{P}_i$'s are the diagonal entries of D, i.e., $D[i, i] = \mathtt{P}_i$. The identity matrix in $\mathcal{M}_m$ is denoted by $\mathtt{I}_m$ and the identity matrix in $\mathcal{M}(n, m)$ is denoted by $I_{m,n}$ which is the same as $\mathtt{I}_{mn}$. If the block matrix $D = Diag(\mathtt{P}, \mathtt{P}, \ldots, \mathtt{P}) \in \mathcal{D}(n, m)$ for some $\mathtt{P} \in GL(m, \mathbb{F}_2)$ then $D = \mathtt{P}I_{m,n}$, and so we simply write $D = Diag(\mathtt{P})$. The zero matrix/vector is denoted by $\mathbf{0}$ with suitable size.

We can interpret a column vector $\mathbf{v} \in \mathbb{F}_2^{mn}$ as a column vector in $(\mathbb{F}_2^m)^n$, say $\mathbf{v} = (\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1})$. The m-block weight $wt_m(\mathbf{v})$ of $\mathbf{v}$ is defined as the number of nonzero component vectors, i.e., $wt_m(\mathbf{v}) = |\{\mathbf{v}_i : \mathbf{v}_i \neq \mathbf{0}, 0 \leq i \leq n - 1\}|$. Let $M \in \mathcal{M}(n, m)$ be a block matrix. The transpose of M denoted by M^T is the usual transpose considering M as an $mn \times mn$ binary matrix, i.e., $M^T[i, j] = M[j, i]^T$. The branch number of a block matrix $M \in \mathcal{M}(n, m)$ is defined as follows.

Definition 1. Let $M \in \mathcal{M}(n, m)$. The *differential branch number* of M is defined as

$$B_d(M) = \min_{\mathbf{v} \neq \mathbf{0}} \{wt_m(\mathbf{v}) + wt_m(M\mathbf{v})\},$$

and the *linear branch number* of M is defined as

$$B_\ell(M) = \min_{\mathbf{v} \neq \mathbf{0}} \{wt_m(\mathbf{v}) + wt_m(M^T\mathbf{v})\}.$$

Similarly, we can also define the branch number of a matrix M of order n over a finite field $\mathbb{F}_{2^m}$ by considering the Hamming weight instead of the m-block weight. It is easy to see that B_d and B_ℓ of any matrix $M \in \mathcal{M}(n,m)$ are less than or equal to $n+1$.

Definition 2. A block matrix $M \in \mathcal{M}(n,m)$ is said to be *MDS* if $B_d(M) = B_\ell(M) = n+1$.

We can also define MDS matrices over finite fields analogously. Evidently, MDS matrices have the maximal branch number. So if the matrix used in a diffusion layer is MDS then a change in a single component of the input vector leads to changes in all the components of the output vector. The following characterization of MDS matrices is an important tool to verify whether a matrix is MDS or not.

Theorem 1. *(See [BR99]) A matrix $M \in \mathcal{M}(n, F_q)$ is* MDS *if and only if every square submatrix of M is nonsingular. Similarly, a block matrix $M \in \mathcal{M}(n,m)$ is* MDS *if and only if every square block submatrix of M is nonsingular.*

The following results can easily be seen from the above theorem.

Lemma 1. *A block matrix $M \in \mathcal{M}(n,m)$ is MDS if and only if its transpose M^T is MDS.*

Lemma 2. *A block matrix $M \in \mathcal{M}(n,m)$ is MDS if and only if its inverse M^{-1} is MDS.*

In many designs of block ciphers, one needs to implement M^{-1} in the decryption if the diffusion layer in the encryption is given by M. In such cases, involutory matrices are more suitable.

Definition 3. A square matrix M is said to be *involutory* if M^2 is equal to the identity matrix. An *involutory MDS matrix* is an MDS matrix which is involutory.

The main advantage of an involutory matrix M is that its inverse is also M. So if an involutory MDS matrix is used in a diffusion layer, then the diffusion layer process is exactly the same in both encryption and decryption.

Next we define various types of matrices that we study in this paper. Specifically, circulant, cyclic, Hadamard, companion and (sparse) DSI matrices are considered. We define these matrices over $\mathcal{M}_m$, and one can easily see the appropriate form of the definitions when such matrices are considered over finite fields.

Definition 4. A *circulant matrix* C of order n over $\mathcal{M}_m$ is a block matrix where each subsequent row is a right rotation by 1 of the previous row. So the matrix C can be determined by its first row, and we denote such a matrix C as $Cir(\mathtt{C}_0, \mathtt{C}_1, \ldots, \mathtt{C}_{n-1})$, where $\mathtt{C}_i$'s are the entries of its first row. The (i,j)-th entry of C can be expressed as $C[i,j] = \mathtt{C}_{(j-i) \bmod n}$.

The diffusion matrix used in the block cipher AES [DR02] is a circulant matrix. One may consider any permutation which is a full cycle instead of the right rotation by 1 as in the case of circulant matrices. In this direction, as a generalization of circulant matrices, cyclic matrices were proposed in [LS16a] which we define below.

Definition 5. Let ρ be a cycle of length n in the permutation group of $\{0, 1, \ldots, n-1\}$. A *cyclic matrix* C_ρ of order n determined by the ordered tuple $(\mathtt{C}_0, \mathtt{C}_1, \ldots, \mathtt{C}_{n-1}) \in [\mathcal{M}_m]^n$ is a block matrix given by $C_\rho[i,j] = \mathtt{C}_{\rho^i(j)}$. We denote such a cyclic matrix C_ρ as $Cyc_\rho(\mathtt{C}_0, \mathtt{C}_1, \ldots, \mathtt{C}_{n-1})$.

The circulant matrices are also cyclic matrices and the corresponding permutation is $\rho = (0\ (n-1)\ (n-2)\ \cdots\ 2\ 1)$, where $\rho = (i_0\, i_1\, \cdots\, i_{n-1})$ means $\rho(i_j) = i_{(j+1) \bmod n}$ for $0 \le j \le n-1$. The number of cycles of length n in the permutation group of $\{0, 1, \ldots, n-1\}$ is $(n-1)!$. The size of the permutation group of $\{1, \ldots, n-1\}$ is also $(n-1)!$. The following result gives a one-to-one correspondence between circulant matrices and cyclic matrices. In the discussion below, the columns/rows of a matrix in $\mathcal{M}(n,m)$ are indexed from 0 to $n-1$.

Lemma 3. *Let ρ be a cycle of length n in the permutation group of $\{0,1,\ldots,n-1\}$. Given a cyclic matrix $C_\rho = Cyc_\rho(\mathtt{C}_0, \mathtt{C}_1, \ldots, \mathtt{C}_{n-1})$ there exists a permutation π of the columns 1 to $n-1$ such that the matrix obtained by applying π on C_ρ is a circulant matrix. Similarly, given a circulant matrix C, any permutation π of the columns 1 to $n-1$ of C gives a cyclic matrix for some cycle ρ of length n in the permutation group of $\{0,1,\ldots,n-1\}$.*

Proof. Let ρ be a cycle of length n in the permutation group of $\{0,1,\ldots,n-1\}$. Note that $\rho^0(0) = 0, \{\rho(0), \rho^2(0), \ldots, \rho^{n-1}(0)\} = \{1,2,\ldots,n-1\}$ and $\rho^{n+j}(0) = \rho^j(0)$ since ρ is a full cycle. Consider the permutation π in the permutation group of $\{1,2,\ldots,n-1\}$ given below in 2-line notation:

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n-1 \\ \rho^{n-1}(0) & \rho^{n-2}(0) & \cdots & \rho(0) \end{pmatrix}.$$

It can easily be seen that the mapping given by $\rho \mapsto \pi$ is a bijection. Let P be the permutation matrix in $\mathcal{P}(n,m)$ corresponding to the extended permutation $\hat{\pi}$ given by $\hat{\pi}(0) = 0$ and $\hat{\pi}(j) = \pi(j)$ for $1 \le j \le n-1$. Now consider $C = C_\rho P$ the matrix obtained by permuting the columns from 1 to $n-1$ of C_ρ corresponding to π. Observe that the column 0 of C and C_ρ are the same and it is given by $[\mathtt{C}_0, \mathtt{C}_{\rho(0)}, \mathtt{C}_{\rho^2(0)}, \ldots, \mathtt{C}_{\rho^{n-1}(0)}]$ as $C_\rho[i,j] = \mathtt{C}_{\rho^i(j)}$. Also observe that the row 0 of C is given by $[\mathtt{C}_0, \mathtt{C}_{\rho^{n-1}(0)}, \mathtt{C}_{\rho^{n-2}(0)}, \ldots, \mathtt{C}_{\rho(0)}]$. Suppose $j = \rho^{i_j}(0)$ for $1 \le j \le n-1$. Then the j-th column of C_ρ and the $(n-i_j)$-th column of C are the same, and it is given by $[\mathtt{C}_{\rho^{i_j}(0)}, \mathtt{C}_{\rho^{i_j+1}(0)}, \ldots, \mathtt{C}_{\rho^{i_j+n-1}(0)}]$. Now by a careful observation we can see that $C = Cir(\mathtt{C}_0, \mathtt{C}_{\rho^{n-1}(0)}, \mathtt{C}_{\rho^{n-2}(0)}, \ldots, \mathtt{C}_{\rho(0)})$, and hence the result. □

The above result can also be derived with a similar argument as in the proof of [LS16a, Theorem 3]. Another important class of matrices is Hadamard matrices defined below.

Definition 6. Let $n = 2^t$. An $n \times n$ block matrix over $\mathcal{M}_m$ is called a *Hadamard matrix* if it can be expressed as follows:

$$H = \begin{bmatrix} H_1 & H_2 \\ H_2 & H_1 \end{bmatrix}$$

where H_1 and H_2 are also Hadamard matrices of order 2^{t-1} over $\mathcal{M}_m$. Note that if the first row of H is given by the ordered tuple $(\mathtt{H}_0, \mathtt{H}_1, \ldots, \mathtt{H}_{2^t-1}) \in [\mathcal{M}_m]^n$ then $H[i,j] = \mathtt{H}_{i \oplus j}$ for $0 \le i, j \le n-1$. We denote such a matrix H as $Had(\mathtt{H}_0, \mathtt{H}_1, \ldots, \mathtt{H}_{2^t-1})$.

There has been a lot of study on the design of lightweight ciphers. In 2011, Guo et al. proposed a new type of matrices known as recursive MDS matrices suitable for lightweight applications [GPP11]. The main idea in their proposal is to use some power of a companion matrix in the diffusion layer. The advantage of a companion matrix is that it can be implemented by an LFSR, and the diffusion layer can be implemented by clocking the LFSR several times.

Definition 7. Let r be a positive integer. A matrix M is said to be *recursive MDS* or *r-MDS* if the matrix M^r is MDS. If M is r-MDS then we say M yields an MDS matrix.

Remark 1. It is easy to see from Lemmas 1 and 2 that if M is r-MDS then M^T and M^{-1} are also r-MDS.

In our work, we consider recursive MDS matrices of the types companion and sparse DSI, and for such a matrix M of order n, the matrix M^r cannot be MDS for $r < n$. If M^r is MDS for $r \ge n$ then the matrix M needs to be applied r times in the serialized implementation of the diffusion layer. So the best case is to see whether M^n is MDS or not. So, in our experiments, we consider recursive MDS matrices that are n-MDS only. Also we say a matrix M is *involutory n-MDS*, if M is n-MDS and M^{2n} is the identity matrix.

Definition 8. A *companion matrix* L associated to the ordered tuple $(\mathtt{L}_0, \mathtt{L}_1, \ldots, \mathtt{L}_{n-1}) \in [\mathcal{M}_m]^n$ is given by

$$L = \begin{pmatrix} \mathbf{0} & \mathtt{I}_m & \mathbf{0} & \ldots & \mathbf{0} \\ \vdots & \vdots & \ddots & & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \ldots & \mathtt{I}_m \\ \mathtt{L}_0 & \mathtt{L}_1 & \mathtt{L}_2 & \ldots & \mathtt{L}_{n-1} \end{pmatrix}.$$

We denote such a matrix L as $Comp(\mathtt{L}_0, \mathtt{L}_1, \ldots, \mathtt{L}_{n-1})$. The matrix L is often associated with the matrix polynomial $\Phi_L(X) = X^n - \mathtt{L}_{n-1}X^{n-1} - \cdots - \mathtt{L}_1 X - \mathtt{L}_0$ since the characteristic polynomial of L is equal to the determinant of $\Phi_L(X)$.

In a recent work [TTKS18], the authors have proposed another type of recursive MDS matrices known as sparse DSI matrices. The definitions presented below are slightly different from the definitions in [TTKS18]. However, as we will see later in Section 3.5 that these matrices are similar and so it is okay to consider in this manner.

Definition 9. Let $n \geq 2$ be an integer. A *Diagonal-Serial Invertible* (DSI) matrix $S = (S[i,j])_{0 \leq i,j \leq (n-1)}$ of order n determined by the ordered tuples $(\mathtt{A}_0, \mathtt{A}_1, \ldots, \mathtt{A}_{n-1}) \in [GL(m, \mathbb{F}_2)]^n$ and $(\mathtt{B}_0, \mathtt{B}_1, \ldots, \mathtt{B}_{n-1}) \in [\mathcal{M}_m]^n$ with $\mathtt{B}_i = \mathbf{0}$ for some $i, 0 \leq i \leq n-1$, is an $n \times n$ block matrix given as follows:

$$S[i,j] = \begin{cases} \mathtt{A}_0, & i = 0, j = n-1 \\ \mathtt{A}_i, & i = j+1 \\ \mathtt{B}_i, & i = j \\ \mathbf{0}, & \text{otherwise.} \end{cases}$$

We denote such a matrix S as $DSI(\mathtt{B}_0, \mathtt{B}_1, \ldots, \mathtt{B}_{n-1}; \mathtt{A}_0, \mathtt{A}_1, \ldots, \mathtt{A}_{n-1})$.

In the above definition, we consider $\mathtt{B}_i = \mathbf{0}$ for some $i, 0 \leq i \leq n-1$, whereas $\mathtt{B}_{n-1} = \mathbf{0}$ in [TTKS18].

Definition 10. Let $n \geq 2$ be an integer and $k = \lfloor \frac{n+1}{2} \rfloor$. A Diagonal-Serial Invertible matrix S of order n determined by the ordered tuples $(\mathtt{A}_0, \mathtt{A}_1, \ldots, \mathtt{A}_{n-1}) \in [GL(m, \mathbb{F}_2)]^n$ and $(\mathtt{B}_0, \mathtt{B}_1, \ldots, \mathtt{B}_{n-1}) \in [\mathcal{M}_m]^n$ is said to sparse or simply *sparse DSI* if $\mathtt{B}_i = \mathbf{0}$ for i odd and $\mathtt{B}_i \in GL(m, \mathbb{F}_2)$ for i even. The (i,j)-th entry of the sparse DSI matrix S is given by

$$S[i,j] = \begin{cases} \mathtt{A}_0, & i = 0, j = n-1 \\ \mathtt{A}_i, & i = j+1 \\ \mathtt{B}_i, & i = j \text{ and even} \\ \mathbf{0}, & \text{otherwise.} \end{cases}$$

We denote such a matrix S with $SpDSI(\mathtt{B}_0, \mathtt{B}_2, \ldots, \mathtt{B}_{2(k-1)}; \mathtt{A}_0, \mathtt{A}_1, \ldots, \mathtt{A}_{n-1})$ as we have $\mathtt{B}_i = \mathbf{0}$ for i odd.

In the above definition, in the case when n is odd, we consider $\mathtt{B}_i = \mathbf{0}$ for i odd, whereas $\mathtt{B}_i = \mathbf{0}$ if $i \in \{1, 3, \ldots, n-4\} \cup \{n-1\}$ in [TTKS18]. In the case when n is even, our definition matches with that of [TTKS18].

The recursive MDS matrices from sparse DSI matrices are of importance due to their low fixed cost in hardware implementation (see Section 2.1). In the case where n is even, the GFS matrices (of suitable order) proposed in [WWW12, Section 5] have the same fixed cost in hardware implementation. We have the following observation on the relation between GFS matrices and sparse DSI matrices.

Remark 2. Let $n = 2k$ and $S = SpDSI(\mathtt{B}_0, \mathtt{B}_2, \ldots, \mathtt{B}_{2(k-1)}; \mathtt{A}_0, \mathtt{A}_1, \ldots, \mathtt{A}_{n-1})$ be a sparse DSI matrix with $\mathtt{A}_i = \mathtt{I}_m$ for i odd. The inverse of the sparse DSI matrix S is a GFS matrix defined in [WWW12, Section 5]. Note that if M is an n-MDS matrix then its inverse M^{-1} is also an n-MDS matrix. So we can view the sparse DSI matrices as a generalization of the GFS matrices proposed in [WWW12, Section 5].

Let $\mathcal{C}(n, m)$ and $\mathcal{H}(n, m)$ denote the set of MDS matrices in $\mathcal{M}(n, m)$ of the type circulant and Hadamard respectively. Also let $\mathcal{L}(n, m)$ and $\mathcal{S}(n, m)$ denote the set of n-MDS matrices in $\mathcal{M}(n, m)$ of the type companion and sparse DSI matrices respectively.

2.1 Hardware Implementation - XOR Count

Suppose that $M \in \mathcal{M}(n, m)$ is an MDS matrix used in a diffusion layer. So the diffusion layer is given by the mapping $\mathbf{v} \mapsto M\mathbf{v}$ for $\mathbf{v} = (\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1}) \in (\mathbb{F}_2^m)^n$. The main component of the computation is $M[i, j]\mathbf{v}_j$ for $0 \leq i, j \leq n-1$, where $\mathbf{v}_j \in \mathbb{F}_2^m$. Essentially, we need to evaluate the cost of hardware implementation of the mapping $\mathbf{u} \mapsto \mathtt{M}\mathbf{u}$ for some $\mathtt{M} \in GL(m, \mathbb{F}_2)$ and $\mathbf{u} \in \mathbb{F}_2^m$. For this purpose, we count the number of XOR gates required in its hardware implementation. There are two metrics proposed in the literature. The direct XOR count was introduced in [KPPY14], and later in [JPST17] another metric known as the sequential XOR count was introduced. We below define both the XOR count metrics. For more details on the two metrics of XOR count, we refer to [Köl19] and references therein.

Definition 11. The direct XOR count (*d-XOR count*) of $\mathtt{M} \in GL(m, \mathbb{F}_2)$ denoted by d-XOR($\mathtt{M}$) is

$$d\text{-XOR}(\mathtt{M}) = \omega(\mathtt{M}) - m,$$

where $\omega(\mathtt{M})$ denotes the number of ones in the matrix $\mathtt{M}$.

Definition 12. Let $\mathtt{M} \in GL(m, \mathbb{F}_2)$ be a nonsingular $m \times m$ binary matrix. The sequential XOR count (*s-XOR count*) of $\mathtt{M}$ denoted by s-XOR($\mathtt{M}$) is equal to ℓ if ℓ is the smallest non-negative integer such that $\mathtt{M}$ can be expressed as

$$\mathtt{M} = \mathtt{P} \prod_{t=1}^{\ell} (\mathtt{I}_m + \mathtt{E}_{i,j})$$

where $\mathtt{P} \in \mathcal{P}_m$ and $\mathtt{E}_{i,j}$, $i \neq j$, is a binary matrix with 1 as (i, j)-th entry and 0 elsewhere.

We have the following result on the XOR counts.

Lemma 4. *([Köl19, Lemma 1]) Let* $\mathtt{M} \in GL(m, \mathbb{F}_2)$. *For any two permutation matrices* $\mathtt{P}$ *and* $\mathtt{Q}$ *in* $\mathcal{P}_m$, *we have*

$$d\text{-XOR}(\mathtt{M}) = d\text{-XOR}(\mathtt{PMQ}) \quad \textit{and} \quad s\text{-XOR}(\mathtt{M}) = s\text{-XOR}(\mathtt{PMQ}).$$

We have $|GL(4, \mathbb{F}_2)| = 20,160$. In Table 1 we present the number of matrices in $GL(4, \mathbb{F}_2)$ with their d-XOR and s-XOR counts.

Table 1: The number of matrices in $GL(4, \mathbb{F}_2)$ with fixed XOR count

XOR count	0	1	2	3	4	5	6	7	8	9
d-XOR count	24	288	1440	3648	4752	4992	2592	1728	600	96
s-XOR count	24	288	2016	7968	8496	1344	24	0	0	0

In the case where the elements of an MDS matrix are from a finite field $\mathbb{F}_q$, we need to implement field element multiplication. We can consider $\mathbb{F}_q$ with $q = 2^m$ as the m-dimensional vector space $\mathbb{F}_2^m$. By distributive property, it can easily be seen that for

$\alpha \in \mathbb{F}_q$, the field element multiplication by α given by $x \mapsto \alpha x$ is a linear function over $\mathbb{F}_2$. For defining the XOR count of $\alpha \in \mathbb{F}_q$, we consider the matrix representation $\mathtt{M}_{\alpha,B}$ of the mapping $x \mapsto \alpha x$ with respect to some basis B of $\mathbb{F}_q$ over $\mathbb{F}_2$.

Definition 13. Let $\alpha \in \mathbb{F}_q$ and B be a basis of $\mathbb{F}_q$ over $\mathbb{F}_2$, where $q = 2^m$. Let $\mathtt{M}_{\alpha,B} \in GL(m, \mathbb{F}_2)$ be the matrix representation of the mapping $x \mapsto \alpha x$ with respect to the basis B. The *d-XOR count* and the *s-XOR count* of α with respect to the basis B, denoted by d-XOR(α, B) and s-XOR(α, B) respectively, is as follows:

$$d\text{-XOR}(\alpha, B) = d\text{-XOR}(\mathtt{M}_{\alpha,B}) \quad \text{and} \quad s\text{-XOR}(\alpha, B) = s\text{-XOR}(\mathtt{M}_{\alpha,B}).$$

Observe that the d/s-XOR count of $\mathtt{M}_{\alpha,B}$ generally differs from the d/s-XOR count of $\mathtt{M}_{\alpha,B'}$ for different bases B and B'. In [BKL16], the authors studied methods to find a basis with which the s-XOR count of a finite field element is optimal.

We use $XOR(\mathtt{A})$ to denote the XOR count of a matrix $\mathtt{A} \in \mathcal{M}_m$ and it can be either the d-XOR count or the s-XOR count of $\mathtt{A}$ unless otherwise mentioned. Note that the circulant (cyclic) MDS and the recursive MDS matrices from the companion or sparse DSI matrices can have a serialized implementation. So the variable cost depends on the elements determining such matrices. The XOR count of these matrices is the number of XOR gates required in one iteration/step of their serialized implementation. Though it is nontrivial to implement Hadamard matrices in a serialized manner, we follow the convention, and consider the cost of implementing its defining elements for the purpose of comparison. We refer to [TTKS18, Section 4.3 & 5] for more details on the XOR count of these matrices. We often use $Cost(M)$ to denote the XOR count of a matrix M. In Table 2 we present XOR counts/Costs of the matrices that we consider (see also [TTKS18, Section 5])

Table 2: XOR count/Cost of various types of matrices

Type of matrix	XOR count/Cost
$Cyc_\rho(\mathtt{C}_0, \mathtt{C}_1, \ldots, \mathtt{C}_{n-1})$	$\sum XOR(\mathtt{C}_i) + (n-1) \cdot m$
$Had(\mathtt{H}_0, \mathtt{H}_1, \ldots, \mathtt{H}_{n-1})$	$\sum XOR(\mathtt{H}_i) + (n-1) \cdot m$
$Comp(\mathtt{L}_0, \mathtt{L}_1, \ldots, \mathtt{L}_{n-1})$	$\sum_{\mathtt{L}_i \mid \forall j < i\, \mathtt{L}_i \neq \mathtt{L}_j} XOR(\mathtt{L}_i) + (n-1) \cdot m$
$SpDSI(\mathtt{B}_0, \mathtt{B}_2, \ldots, \mathtt{B}_{2(k-1)}; \mathtt{A}_0, \ldots, \mathtt{A}_{n-1})$	$\sum XOR(\mathtt{A}_i) + \sum_{\mathtt{B}_i \neq \mathtt{A}_{(i+1) \bmod n}} XOR(\mathtt{B}_i) + k \cdot m$

where $k = \lfloor \frac{n+1}{2} \rfloor$.

The last component in the entries of the second column in Table 2 gives the fixed cost of the corresponding matrices, and it depends on the size of the matrix but not on the entries of the matrix. Note that the fixed cost of sparse DSI matrices is close to half the cost of other matrix types of the same order.

Next we discuss conjugacy classes and restricted conjugacy classes. These classes play an important role in the exhaustive search for MDS matrices which we discuss in Section 3.

2.2 Conjugacy Classes and Restricted Conjugacy Classes

Let $\mathcal{G} = GL(m, \mathbb{F}_q)$ be the general linear group of order m over $\mathbb{F}_q$. For $\mathtt{A}, \mathtt{B} \in \mathcal{G}$, we say $\mathtt{A}$ is similar to $\mathtt{B}$ or $\mathtt{A} \sim \mathtt{B}$ if there exists $\mathtt{P} \in \mathcal{G}$ such that $\mathtt{B} = \mathtt{P}^{-1}\mathtt{A}\mathtt{P}$. It is well known that the similarity relation is an equivalence relation on $\mathcal{G}$. A related concept in group theory is $\mathcal{G}$ acting on itself by conjugation. And so the equivalence classes are known as conjugacy classes. For $\mathtt{A} \in \mathcal{G}$, the orbit or *conjugacy class* containing $\mathtt{A}$ is given by

$$cc(\mathtt{A}) = \{\mathtt{P}^{-1}\mathtt{A}\mathtt{P} : \mathtt{P} \in \mathcal{G}\}.$$

Let $\mathcal{N}_{\mathcal{G}}$ denote a set of representatives of the distinct conjugacy classes.

Lemma 5. *[Sta12, p. 138] The number of distinct conjugacy classes in the group $\mathcal{G} = GL(4, \mathbb{F}_q)$ is given by*

$$|\mathcal{N}_{\mathcal{G}}| = q^4 - q.$$

The centralizer of an element $\mathtt{A} \in \mathcal{G}$ is defined by

$$\mathcal{C}_{\mathcal{G}}(\mathtt{A}) = \{\mathtt{P} \in \mathcal{G} : \mathtt{P}^{-1}\mathtt{AP} = \mathtt{A}\}.$$

It is also well known that $\mathcal{C}_{\mathcal{G}}(\mathtt{A})$ forms a subgroup of $\mathcal{G}$. Now consider the action of $\mathcal{C}_{\mathcal{G}}(\mathtt{A})$ on $\mathcal{G}$ by conjugation. For $\mathtt{B}, \mathtt{C} \in \mathcal{G}$, we say $\mathtt{B} \sim_{\mathtt{A}} \mathtt{C}$ if there exists $\mathtt{P} \in \mathcal{C}_{\mathcal{G}}(\mathtt{A})$ such that $\mathtt{C} = \mathtt{P}^{-1}\mathtt{BP}$. It is easy to see that this is an equivalence relation. We call these equivalence classes as $\mathtt{A}$-restricted conjugacy classes. For $\mathtt{A} \in \mathcal{G}$, the $\mathtt{A}$-*restricted conjugacy class* containing $\mathtt{B} \in \mathcal{G}$ is given by

$$cc_{\mathtt{A}}(\mathtt{B}) = \{\mathtt{P}^{-1}\mathtt{BP} : \mathtt{P} \in \mathcal{C}_{\mathcal{G}}(\mathtt{A})\}.$$

Let $\mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$ denote a set of representatives of the distinct $\mathtt{A}$-restricted conjugacy classes.

For the case where $\mathcal{G} = GL(4, \mathbb{F}_2)$, we present below a set $\mathcal{N}_{\mathcal{G}}$ and the sizes of $\mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$ for $\mathtt{A} \in \mathcal{N}_{\mathcal{G}}$. Note that by Lemma 5 we have $|\mathcal{N}_{\mathcal{G}}| = 14$. In the table below we represent a matrix $\mathtt{A} \in \mathcal{G} = GL(4, \mathbb{F}_2)$ given by

$$\mathtt{A} = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{bmatrix} \tag{1}$$

by the integer value $\sum_{i=0}^{15} a_i 2^i$ in hexadecimal form. For example the identity matrix $\mathtt{I} \in \mathcal{G}$ is represented by `0x8421`.

Table 3: The number of elements in $\mathtt{A}$-restricted conjugacy classes : $|\mathcal{N}_{\mathcal{G}}^{\mathtt{A}}|$ for $\mathtt{A} \in \mathcal{N}_{\mathcal{G}}$

$\mathtt{A} \in \mathcal{N}_{\mathcal{G}}$	0x1842	0x1843	0x1846	0x2816	0x2841	0x2853	0x42c1
$\lvert cc(\mathtt{A})\rvert$	2520	1344	1344	1680	1120	1344	2880
$\lvert\mathcal{C}_{\mathcal{G}}(\mathtt{A})\rvert$	8	15	15	12	18	15	7
$\lvert\mathcal{N}_{\mathcal{G}}^{\mathtt{A}}\rvert$	2572	1380	1380	1740	1198	1380	2886
$\mathtt{A} \in \mathcal{N}_{\mathcal{G}}$	0x4812	0x4813	0x4821	0x4c13	0x8143	0x8243	0x8421
$\lvert cc(\mathtt{A})\rvert$	210	3360	105	112	2880	1260	1
$\lvert\mathcal{C}_{\mathcal{G}}(\mathtt{A})\rvert$	96	6	192	180	7	16	20160
$\lvert\mathcal{N}_{\mathcal{G}}^{\mathtt{A}}\rvert$	268	3400	149	154	2886	1340	14

Observe that $|cc(\mathtt{A})| \cdot |\mathcal{C}_{\mathcal{G}}(\mathtt{A})| = |\mathcal{G}|$ for $\mathtt{A} \in \mathcal{G}$. The numbers in Table 3 do not depend on the choice of representatives $\mathcal{N}_{\mathcal{G}}$. We now present our main results in the next section.

3 Exhaustive Search for MDS Matrices

If a circulant matrix $C \in \mathcal{M}(n, m)$ is MDS then all the entries must be nonsingular. In a naive approach, in order to exhaustively search for circulant MDS matrices, the number of candidates for that we need to verify the MDS property is $|GL(m, \mathbb{F}_2)|^n$, which is practically difficult for $m = 4$ and $n \geq 4$. Note that $|GL(4, \mathbb{F}_2)| = 20,160 > 2^{14}$. It is the same for other types of matrices as well. In this section we first present some basic results without proofs. By using these basic results and the results on the conjugacy classes, we are able to reduce the search domain. In order to exhaustively search for circulant MDS

matrices, it is enough to search for circulant MDS matrices in this reduced domain. We also apply some space-time trade-off techniques to speed up the search/computation. For given parameters and the type of matrix, from the MDS matrices in the reduced search domain, one can easily get all the MDS matrices of that type. Next we present some basic results on the similarity/equivalence of (recursive) MDS matrices.

Definition 14. Two matrices M and M' in $\mathcal{M}(n,m)$ are called *diagonal equivalent*, denoted by $M \sim_{de} M'$, if there exist two diagonal matrices $P, Q \in \mathcal{D}(n,m)$ such that $M' = PMQ$.

Lemma 6. *Suppose that two matrices M and M' in $\mathcal{M}(n,m)$ are diagonal equivalent. Then M is MDS if and only if M' is MDS.*

Definition 15. Two matrices M and M' in $\mathcal{M}(n,m)$ are called *diagonal similar*, denoted by $M \sim_{ds} M'$, if there exists a block diagonal matrix $P \in \mathcal{D}(n,m)$ such that $M' = P^{-1}MP$.

Lemma 7. *Suppose that two matrices M and M' in $\mathcal{M}(n,m)$ are diagonal similar. Then M is r-MDS if and only if M' is r-MDS.*

Definition 16. Two matrices M and M' in $\mathcal{M}(n,m)$ are called *permutation equivalent*, denoted by $M \sim_{pe} M'$, if there exist two permutation matrices $P, Q \in \mathcal{P}(n,m)$ such that $M' = PMQ$.

Lemma 8. *Suppose that two matrices M and M' in $\mathcal{M}(n,m)$ are permutation equivalent. Then M is MDS if and only if M' is MDS.*

Definition 17. Two matrices M and M' in $\mathcal{M}(n,m)$ are called *permutation similar*, denoted by $M \sim_{ps} M'$, if there exists a permutation matrix $P \in \mathcal{P}(n,m)$ such that $M' = P^{-1}MP$.

Lemma 9. *Suppose that two matrices M and M' in $\mathcal{M}(n,m)$ are permutation similar. Then M is r-MDS if and only if M' is r-MDS.*

Similarly, we can also define diagonal/permutation equivalence/similarity for matrices in $\mathcal{M}(n, \mathbb{F}_q)$, and one can easily see that Lemmas 6 to 9 are also valid for this case.

If the matrix $M \in \mathcal{M}(n,m)$ is MDS then it is necessary that all the 2×2 block submatrices of M are nonsingular. The number of 2×2 block submatrices of M is given by $\binom{n}{2}^2$. It may happen that, some of these submatrices are multiples of another submatrix by block permutation matrices. By the following result, it is possible to reduce the number of 2×2 submatrices that we need to verify the nonsingularity and thus we can avoid some unnecessary checks.

Lemma 10. *Let $M \in \mathcal{M}(n,m)$ be an $n \times n$ block matrix over $\mathcal{M}_m$. Let $P, Q \in \mathcal{P}(n,m)$ be permutation matrices. The matrix M is nonsingular if and only if PMQ is nonsingular. In particular, if*

$$M = \begin{pmatrix} \mathtt{A} & \mathtt{B} \\ \mathtt{C} & \mathtt{D} \end{pmatrix}$$

is nonsingular then RM, MR and RMR are also nonsingular, where

$$R = \begin{pmatrix} \mathbf{0} & \mathtt{I}_m \\ \mathtt{I}_m & \mathbf{0} \end{pmatrix}.$$

To verify the nonsingularity of 2×2 block matrices, we use the following result.

Lemma 11. *Suppose that*

$$M = \begin{pmatrix} \mathtt{A} & \mathtt{B} \\ \mathtt{C} & \mathtt{D} \end{pmatrix}$$

is a 2×2 block matrix over $GL(m, \mathbb{F}_2)$. Then we have M is nonsingular if and only if $(\mathtt{A} + \mathtt{B}\mathtt{D}^{-1}\mathtt{C})$ is nonsingular.

To verify the nonsingularity of higher order block submatrices, we use the recursive formulas given in [Pow11]. In particular, we use the formula given in [Pow11, Section 4.2] for 3×3 block matrices.

Let $\mathcal{G} = GL(m, \mathbb{F}_2)$ and $\mathcal{N}_\mathcal{G}$ denote a set of representatives of the distinct conjugacy classes. For $\mathtt{A} \in \mathcal{N}_\mathcal{G}$, let $\mathcal{N}_\mathcal{G}^\mathtt{A}$ denote a set of representatives of the distinct $\mathtt{A}$-restricted conjugacy classes. Recall that, for $\mathtt{P} \in \mathcal{G}$, the block diagonal matrix $Diag(\mathtt{P}) = \mathtt{P}I_{m,n}$. Next we discuss our technique to reduce the search space using conjugacy classes and restricted conjugacy classes. The results are presented in a more general form, but for the experimental results we consider $m = 4$ and the order n of the matrices will be specified.

3.1 Circulant Matrices

In this section we consider circulant matrices over $\mathcal{M}_m$. In order to perform exhaustive search, we first reduce the search space using conjugacy/restricted conjugacy classes.

Theorem 2. *Let $i, j, k \in \{0, 1, \ldots, n-1\}$ be distinct integers. For any circulant MDS matrix $C = Cir(\mathtt{C}_0, \mathtt{C}_1, \ldots, \mathtt{C}_{n-1}) \in \mathcal{C}(n, m)$ there exists $\mathtt{P}, \mathtt{Q} \in GL(m, \mathbb{F}_2)$ such that $C = Diag(\mathtt{P})C'Diag(\mathtt{Q})$, where $C' = Cir(\mathtt{C}'_0, \mathtt{C}'_1, \ldots, \mathtt{C}'_{n-1}) \in \mathcal{C}(n, m)$ is a circulant MDS matrix with $\mathtt{C}'_i = \mathtt{I}_m, \mathtt{C}'_j = \mathtt{A}$ for some $\mathtt{A} \in \mathcal{N}_\mathcal{G}$ and $\mathtt{C}'_k = \mathtt{B}$ for some $\mathtt{B} \in \mathcal{N}_\mathcal{G}^\mathtt{A}$.*

Proof. First note that the product of a circulant matrix and a block diagonal matrix of the form $Diag(\mathtt{P})$ is a circulant matrix. Let us consider $\mathtt{P}_1 = \mathtt{C}_i^{-1}$. Suppose that $\mathtt{P}_1\mathtt{C}_j \in cc(\mathtt{A})$ for some $\mathtt{A} \in \mathcal{N}_\mathcal{G}$. Then there exists a matrix $\mathtt{P}_2 \in \mathcal{G} = GL(m, \mathbb{F}_2)$ such that $\mathtt{P}_1\mathtt{C}_j = \mathtt{P}_2\mathtt{A}\mathtt{P}_2^{-1}$. Now consider the matrix

$$C_1 = Diag(\mathtt{P}_2^{-1})Diag(\mathtt{P}_1)CDiag(\mathtt{P}_2).$$

Observe that we have $C_1[0, i] = \mathtt{I}_m$ and $C_1[0, j] = \mathtt{A}$. Suppose that $C_1[0, k] \in cc_\mathtt{A}(\mathtt{B})$ for some $\mathtt{B} \in \mathcal{N}_\mathcal{G}^\mathtt{A}$. Then there exists $\mathtt{P}_3 \in \mathcal{C}_\mathcal{G}(\mathtt{A})$ such that $C_1[0, k] = \mathtt{P}_3\mathtt{B}\mathtt{P}_3^{-1}$. Note that $\mathtt{P}_3^{-1}C_1[0, j]\mathtt{P}_3 = \mathtt{P}_3^{-1}\mathtt{A}\mathtt{P}_3 = \mathtt{A}$ since $\mathtt{P}_3 \in \mathcal{C}_\mathcal{G}(\mathtt{A})$ and $\mathtt{P}_3^{-1}\mathtt{P}_2^{-1}\mathtt{P}_1C[0, k]\mathtt{P}_2\mathtt{P}_3 = \mathtt{B}$. We take $\mathtt{Q} = \mathtt{P}_3^{-1}\mathtt{P}_2^{-1}$ and $\mathtt{P} = \mathtt{P}_1^{-1}\mathtt{Q}^{-1}$, and it is easy to see that

$$C' = Diag(\mathtt{P}^{-1})CDiag(\mathtt{Q}^{-1})$$

is in the required form. By Lemma 6 we can see that the matrix C' is MDS. □

Observe that in order to search for circulant MDS matrices of order n over $\mathcal{M}_m$, it is enough to search for circulant MDS matrices of the form C' given in Theorem 2. We have $\mathtt{C}'_i = \mathtt{I}_m$, $\mathtt{C}'_j = \mathtt{A} \in \mathcal{N}_\mathcal{G}$ and $\mathtt{C}'_k = \mathtt{B} \in \mathcal{N}_\mathcal{G}^\mathtt{A}$. We can then get all the solutions C by $C = Diag(\mathtt{P}^{-1})C'Diag(\mathtt{Q}^{-1})$, where $\mathtt{P}, \mathtt{Q} \in GL(m, \mathbb{F}_2)$.

We now illustrate the main ideas of our search technique considering the case of circulant matrices of order 8 over $\mathcal{G} = GL(4, \mathbb{F}_2)$. Let $C = Cir(\mathtt{C}_0, \mathtt{C}_1, \ldots, \mathtt{C}_7)$ be a circulant matrix of order 8 over $GL(4, \mathbb{F}_2)$. In our search, we choose $\mathtt{C}_0 = \mathtt{I}_4$, $\mathtt{C}_4 = \mathtt{A} \in \mathcal{N}_\mathcal{G}$, $\mathtt{C}_2 = \mathtt{B} \in \mathcal{N}_\mathcal{G}^\mathtt{A}$ and $\mathtt{C}_i \in GL(4, \mathbb{F}_2)$ for $i \in \{1, 3, 5, 6, 7\}$. We first collect all the distinct 2×2 submatrices of C that we need to check nonsingularity to verify the MDS property of C. We eliminate unnecessary checks by using Lemma 10. In fact, we need to check the nonsingularity of 100 distinct 2×2 submatrices of C in this case. We have

$$M = \begin{pmatrix} \mathtt{C}_0 & \mathtt{C}_4 \\ \mathtt{C}_4 & \mathtt{C}_0 \end{pmatrix}$$

as a 2×2 submatrix of C. So we have exactly 5 choices for $\mathtt{C}_4$ such that the matrix M is nonsingular (need to verify whether $\mathtt{I}_4 + \mathtt{C}_4^2$ is nonsingular or not). We have 7 submatrices of order 2 involving $\mathtt{C}_2, \mathtt{C}_6$ and $\mathtt{C}_4$. For a fixed choice of $\mathtt{C}_4$, we verify whether these 7 submatrices are nonsingular or not. We store all the choices of $\mathtt{C}_2, \mathtt{C}_6$ that satisfy the

required conditions in a list for later use. We have 5 submatrices of order 2 involving $\mathtt{C}_1, \mathtt{C}_5$ and $\mathtt{C}_4$ (also with $\mathtt{C}_3, \mathtt{C}_7$ and $\mathtt{C}_4$). For a fixed choice of $\mathtt{C}_4$, we create lists for valid choices of the pairs $(\mathtt{C}_1, \mathtt{C}_5)$ and $(\mathtt{C}_3, \mathtt{C}_7)$ satisfying the required nonsingularity conditions. We now proceed to verify the nonsingularity of the other 2×2 submatrices. By creating lists, we are able to substantially reduce the number of candidates that we need to verify the remaining conditions. In verifying the remaining conditions, in the process, if we encounter a singular submatrix then we exit permanently and move on to verify the next candidate. Finally we prepare a list of potential candidates C satisfying that all the 2×2 submatrices of C are nonsingular. Now we verify the determinants of submatrices of order ≥ 3 recursively by using the formulas in [Pow11]. As usual, in the process of verification, if we encounter a singular submatrix, we then exit permanently and move on to verify the next candidate. Since $\mathtt{C}_0 = \mathtt{I}_4$ and few choices for $\mathtt{C}_4$, from the conditions on the 2×2 submatrices, we see that the number of candidates that we actually need to verify the nonsingularity of higher order submatrices is significantly less, and so it is possible to complete the exhaustive search on a desktop computer quickly.

From the solution set in the restricted domain, we eliminate (few) duplicates in the sense that no two matrices are constant diagonal similar. In this way, we get 32 distinct circulant MDS matrices of order $n = 8$ up to (constant) diagonal similarity, and we denote it by $\mathcal{C}^r(8, 4)$. Now we extend it by considering matrices of the form $C' = Diag(\mathtt{P})^{-1} C Diag(\mathtt{P})$ for $C \in \mathcal{C}^r(8, 4)$ and $\mathtt{P} \in GL(4, \mathbb{F}_2)$, and we denote the extended set by $\mathcal{C}^{re}(8, 4)$. In this way, we get $\mathcal{C}^{re}(8, 4) = 645,120$ distinct circulant MDS matrices. Note that the diagonal element of the matrices in $\mathcal{C}^{re}(8, 4)$ is equal to $\mathtt{I}_4$. Observe that any matrix C in $\mathcal{C}(8, 4)$ satisfies $C = Diag(\mathtt{Q})C'$ for some $C' \in \mathcal{C}^{re}(8, 4)$ and $\mathtt{Q} \in GL(4, \mathbb{F}_2)$. Therefore we have

$$|\mathcal{C}(8, 4)| = |\mathcal{C}^{re}(8, 4)| \cdot |GL(4, \mathbb{F}_2)|.$$

Next we present our experimental results for $n = 4, 5, 6, 7$. In the case $n = 4$ we consider $\mathtt{C}_0 = \mathtt{I}_4$, $\mathtt{C}_2 = \mathtt{A} \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{C}_1 = \mathtt{B} \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. In this case we have $\mathtt{C}_2 \neq \mathtt{I}_4$. We get $|\mathcal{C}^r(4, 4)| = 852$ and $|\mathcal{C}^{re}(4, 4)| = 6,875,904$.

In the case $n = 5$ we consider $\mathtt{C}_0 = \mathtt{I}_4$, $\mathtt{C}_3 = \mathtt{A} \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{C}_2 = \mathtt{B} \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. If $\mathtt{C}_3 = \mathtt{I}_4$ then we consider $\mathtt{C}_2 = \mathtt{A} \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{C}_1 = \mathtt{B} \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. We get $|\mathcal{C}^r(5, 4)| = 1,485$ and $|\mathcal{C}^{re}(5, 4)| = 2,829,120$.

In the case $n = 6$ we consider $\mathtt{C}_0 = \mathtt{I}_4$, $\mathtt{C}_3 = \mathtt{A} \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{C}_2 = \mathtt{B} \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. In this case we have $\mathtt{C}_3 \neq \mathtt{I}_4$. We get $|\mathcal{C}^r(6, 4)| = 54$ and $|\mathcal{C}^{re}(6, 4)| = 169,344$.
From the experimental results, we have the following observations:

1. There is no circulant/cyclic MDS matrix of order 7 over $GL(4, \mathbb{F}_2)$.
2. There is no involutory circulant/cyclic MDS matrix of order $6, 8$ over $GL(4, \mathbb{F}_2)$.
3. There is no circulant MDS matrix of order 8 over $\mathbb{F}_{2^4}$ but there exist circulant MDS matrices of order 8 over $GL(4, \mathbb{F}_2)$.

The problem of constructing involutory circulant MDS matrices over $GL(4, \mathbb{F}_2)$ of order $6, 8$ was mentioned in [LW16, Problem 1]. But we have a negative result. In fact, by using Lemma 3 we have verified that there is no involutory cyclic MDS matrix of order $6, 8$ over $GL(4, \mathbb{F}_2)$. For this purpose, it is enough to verify the involutory property of cyclic matrices of the form $\hat{C} = CDiag(\mathtt{Q})P$ for $C \in \mathcal{C}^r(n, 4)$, $\mathtt{Q} \in GL(4, \mathbb{F}_2)$, and $P \in \mathcal{P}(n, m)$ with $P[0, 0] = \mathtt{I}_m$.

We have the following result on the permutation equivalence of circulant MDS matrices.

Lemma 12. *[LS16a, Lemma 1] Let $C = Cir(\mathtt{C}_0, \mathtt{C}_1, \ldots, \mathtt{C}_{n-1})$ be a circulant matrix over $\mathcal{M}_m$ and let $C^\sigma = Cir(\mathtt{C}_{\sigma(0)}, \mathtt{C}_{\sigma(1)}, \ldots, \mathtt{C}_{\sigma(n-1)})$ for some permutation σ. Then we have $C \sim_{pe} C^\sigma$ if and only if the permutation σ satisfies $\sigma(i) = (bi + a) \bmod n$ for $0 \leq i \leq n-1$, where $a, b \in \mathbb{Z}_n$ with $\gcd(b, n) = 1$.*

Remark 3. The number of permutations σ satisfying the condition in Lemma 12 is given by $n\phi(n)$, where $\phi(n)$ is Euler's totient function. For each such σ, we can see by Lemma 8 that C is MDS if and only if C^σ is MDS. So given a circulant MDS matrix $C \in \mathcal{C}(n,m)$, we can generate up to $n\phi(n)$ many matrices in $\mathcal{C}(n,m)$. Since the defining elements of all such matrices are the same, the cost/XOR count of all those matrices are the same.

By Lemma 4 we get the following result.

Lemma 13. *Let C be a circulant MDS matrix over $\mathcal{M}_m$. Then for $P = Diag(\mathtt{P})$ and $Q = Diag(\mathtt{Q})$, where $\mathtt{P}, \mathtt{Q} \in \mathcal{P}_m$ are permutation matrices of order m, we have*

$$Cost(C) = Cost(PCQ).$$

In particular,

$$Cost(C) = Cost(P^{-1}CP).$$

We compute the cost of the matrices in $\mathcal{C}(n,4)$ according to the formula given in Table 2. We get a list of matrices with the least cost with respect to both d-XOR and s-XOR metrics. By reverse process, we get a base set of circulant MDS matrices with the least cost in the sense that by applying Lemmas 12 and 13 we get all the circulant MDS matrices with the same cost.

In the appendix we present a base set of (involutory) circulant MDS matrices in $\mathcal{C}(n,4)$ with the least cost (according to the formula in Table 2) from which we can generate all the circulant MDS matrices with the same cost.

3.2 Hadamard Matrices

In this section we consider Hadamard matrices over $\mathcal{M}_m$. With a similar argument as in the proof of Theorem 2 we get the following result in the case of Hadamard MDS matrices from which we can reduce the search space.

Theorem 3. *Let $i, j, k \in \{0, 1, \ldots, n-1\}$ be distinct integers. For any Hadamard MDS matrix $H = Had(\mathtt{H}_0, \mathtt{H}_1, \ldots, \mathtt{H}_{n-1}) \in \mathcal{H}(n,m)$ there exists $\mathtt{P}, \mathtt{Q} \in GL(m, \mathbb{F}_2)$ such that $H = Diag(\mathtt{P})H'Diag(\mathtt{Q})$, where $H' = Had(\mathtt{H}'_0, \mathtt{H}'_1, \ldots, \mathtt{H}'_{n-1}) \in \mathcal{H}(n,m)$ is a Hadamard MDS matrix with $\mathtt{H}'_i = \mathtt{I}_m, \mathtt{H}'_j = \mathtt{A}$ for some $\mathtt{A} \in \mathcal{N}_\mathcal{G}$ and $\mathtt{H}'_k = \mathtt{B}$ for some $\mathtt{B} \in \mathcal{N}_\mathcal{G}^\mathtt{A}$.*

We have the following result on the equivalence classes of Hadamard matrices.

Lemma 14. *[LS16b, Theorem 5] Let $H = Had(\mathtt{H}_0, \mathtt{H}_1, \ldots, \mathtt{H}_{n-1})$ be a Hadamard matrix over $\mathcal{M}_m$ and let $H^\sigma = Had(\mathtt{H}_{\sigma(0)}, \mathtt{H}_{\sigma(1)}, \ldots, \mathtt{H}_{\sigma(n-1)})$ for some permutation σ. Then we have $H \sim_{pe} H^\sigma$ if and only if the permutation σ satisfies $\sigma(i \oplus j) = \sigma(i) \oplus \sigma(j) \oplus \sigma(0)$ for $0 \le i, j \le n-1$.*

Remark 4. Let $n = 2^t$ for some $t > 0$. The number of permutations σ satisfying the condition in Lemma 14 is given by $n \cdot |GL(t, \mathbb{F}_2)|$. For each such σ, by Lemma 8 we have H is MDS if and only if H^σ is MDS. Also note that the defining elements are distinct in a Hadamard MDS matrix. So given a Hadamard MDS matrix $H \in \mathcal{H}(n,m)$, we can generate $n \cdot |GL(t, \mathbb{F}_2)|$ many matrices in $\mathcal{H}(n,m)$. Since the defining elements of all such matrices are the same, the XOR counts of all those matrices are the same.

We now present our experimental results.

Case: $n = 4$

Let $H = Had(\mathtt{H}_0, \mathtt{H}_1, \mathtt{H}_2, \mathtt{H}_3)$. In our search we consider $\mathtt{H}_0 = \mathtt{I}_4$, $\mathtt{H}_1 = \mathtt{A} \in \mathcal{N}_\mathcal{G}$ and $\mathtt{H}_2 \in \mathcal{N}_\mathcal{G}^\mathtt{A}$. Note that if H is MDS then $\mathtt{H}_i \neq \mathtt{H}_j$ for $i \neq j$. So we have $\mathtt{H}_1 \neq \mathtt{I}_4$. This way we get 560 distinct Hadamard MDS matrices up to (constant) diagonal similarity, and we denote it by $\mathcal{H}^r(4,4)$. Now we extend it by considering matrices of the form $H' = Diag(\mathtt{P})^{-1}HDiag(\mathtt{P})$ for $H \in \mathcal{H}^r(4,4)$ and $\mathtt{P} \in GL(4, \mathbb{F}_2)$, and we denote the extended set by $\mathcal{H}^{re}(4,4)$. In

this way, we get $\mathcal{H}^{re}(4,4) = 2,376,912$ distinct Hadamard MDS matrices. Note that the diagonal element of the matrices in $\mathcal{H}^{re}(4,4)$ is equal to $\mathtt{I}_4$. Observe that any matrix in $\mathcal{H}(4,4)$ is a constant multiple of a matrix in $\mathcal{H}^{re}(4,4)$. Therefore we have

$$|\mathcal{H}(4,4)| = |\mathcal{H}^{re}(4,4)| \cdot |GL(4,\mathbb{F}_2)|.$$

Case: $n = 8$
Let $H = Had(\mathtt{H}_0, \mathtt{H}_1, \mathtt{H}_2, \ldots, \mathtt{H}_7)$. We choose the index choices same as above. In this case, we get 336 distinct matrices up to (constant) diagonal similarity, and we denote it by $\mathcal{H}^r(8,4)$. Similarly, we get $|\mathcal{H}^{re}(8,4)| = 451,584$ distinct Hadamard MDS matrices, where the diagonal element in these matrices is equal to $\mathtt{I}_4$.

In the appendix we present a base set of (involutory) Hadamard MDS matrices in $\mathcal{H}(n,4)$ for $n = 4, 8$ with the least cost (according to the formula in Table 2) from which we can generate all the Hadamard MDS matrices with the same cost.

3.3 Recursive MDS Matrices from Companion Matrices

In this section we consider companion matrices over $\mathcal{M}_m$. We first present a result from which we can reduce the search space. Then we present our experimental results on the exhaustive search for 4-MDS companion matrices of order 4 over $GL(4,\mathbb{F}_2)$.

Theorem 4. *Let $i, j \in \{0, 1, \ldots, n-1\}$ be distinct integers. For any recursive MDS matrix $L = Comp(\mathtt{L}_0, \mathtt{L}_1, \ldots, \mathtt{L}_{n-1}) \in \mathcal{L}(n,m)$ there exists $\mathtt{P} \in GL(m,\mathbb{F}_2)$ such that $L = Diag(\mathtt{P})^{-1} L' Diag(\mathtt{P})$, where $L' = Comp(\mathtt{L}'_0, \mathtt{L}'_1, \ldots, \mathtt{L}'_{n-1}) \in \mathcal{L}(n,m)$ is a recursive MDS matrix with $\mathtt{L}'_i = \mathtt{A}$ for some $\mathtt{A} \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{L}'_j = \mathtt{B}$ for some $\mathtt{B} \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$.*

Proof. Let L be a companion matrix as given above. First note that $Diag(\mathtt{P})LDiag(\mathtt{P})^{-1}$ is also a companion matrix. Suppose that $\mathtt{L}_i \in cc(\mathtt{A})$ for some $\mathtt{A} \in \mathcal{N}_{\mathcal{G}}$. Then there exists a matrix $\mathtt{P}_1 \in \mathcal{G} = GL(m,\mathbb{F}_2)$ such that $\mathtt{L}_i = \mathtt{P}_1 \mathtt{A} \mathtt{P}_1^{-1}$. Now consider the matrix

$$L_1 = Diag(\mathtt{P}_1^{-1}) L Diag(\mathtt{P}_1).$$

Observe that we have $L_1[n-1, i] = \mathtt{A}$. Suppose that $L_1[n-1, j] \in cc_{\mathtt{A}}(\mathtt{B})$ for some $\mathtt{B} \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. Then there exists $\mathtt{P}_2 \in \mathcal{C}_{\mathcal{G}}(\mathtt{A})$ such that $L_1[n-1, j] = \mathtt{P}_2 \mathtt{B} \mathtt{P}_2^{-1}$. Note that $\mathtt{P}_2^{-1} L_1[n-1, i] \mathtt{P}_2 = \mathtt{P}_2^{-1} \mathtt{A} \mathtt{P}_2 = \mathtt{A}$ since $\mathtt{P}_2 \in \mathcal{C}_{\mathcal{G}}(\mathtt{A})$. We take $\mathtt{P} = \mathtt{P}_2^{-1} \mathtt{P}_1^{-1}$, and it is easy to see that

$$L' = Diag(\mathtt{P}) L Diag(\mathtt{P}^{-1})$$

is in the required form. By Lemma 7 we can see that the matrix L' is recursive MDS. □

We now present our experimental results for the case where $n = m = 4$. In our search we first consider $\mathtt{L}_0 = \mathtt{A} (\neq \mathtt{I}_4) \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{L}_2 \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. In the case when $\mathtt{L}_0 = \mathtt{I}_4$, we consider $\mathtt{L}_2 = \mathtt{A} \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{L}_1 \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. In this way, we get $1,495$ distinct matrices up to (constant) diagonal similarity, and we denote it by $\mathcal{L}^r(4,4)$. Now we extend it by considering matrices of the form $L' = Diag(\mathtt{P})^{-1} L Diag(\mathtt{P})$ for $L \in \mathcal{L}^r(4,4)$ and $\mathtt{P} \in GL(4,\mathbb{F}_2)$, and observe that the extended set is $\mathcal{L}(4,4)$. In this way, we get $|\mathcal{L}(4,4)| = 7,358,400$ distinct 4-MDS companion matrices of order 4 over $GL(4,\mathbb{F}_2)$.

It is well known that there is no companion matrix over fields of even characteristic which yields an involutory MDS matrix (see [GPV19, Theorem 2]). But we get involutory MDS matrices from $\mathcal{L}(4,4)$. We provide such a matrix in the appendix. Now we state this result.

Theorem 5. *There exists a companion matrix L of order 4 over $GL(4,\mathbb{F}_2)$ such that L^4 is involutory MDS.*

In the appendix we present a base set of companion matrices in $\mathcal{L}(4,4)$ with the least cost (according to the formula in Table 2) from which we can generate all the companion matrices with the same cost.

3.4 Recursive MDS Matrices from Sparse DSI Matrices

In this section we consider sparse DSI matrices over $\mathcal{M}_m$. This problem was mentioned in [TTKS18, Section 7.2]. We first present a result from which we can reduce the search space. Then we show a close relationship between sparse DSI matrices and Ring LFSRs. Next we present our experimental results on the exhaustive search for n-MDS sparse DSI matrices of order n over $GL(4, \mathbb{F}_2)$ for $n = 4, 5, 6, 7, 8$.

Theorem 6. *Let $n \geq 2$ be an integer and $k = \lfloor \frac{n+1}{2} \rfloor$. Let t be an even integer with $0 \leq t \leq n-1$. For any recursive MDS matrix $S = SpDSI(\mathtt{B}_0, \mathtt{B}_2, \ldots, \mathtt{B}_{2(k-1)}; \mathtt{A}_0, \mathtt{A}_1, \ldots, \mathtt{A}_{n-1}) \in \mathcal{S}(n, m)$ there exists $D = Diag(\mathtt{P}_0, \mathtt{P}_1, \ldots, \mathtt{P}_{n-1}) \in \mathcal{D}(n, m)$ such that $S = D^{-1}S'D$, where $S' = SpDSI(\mathtt{B}'_0, \mathtt{B}'_2, \ldots, \mathtt{B}'_{2(k-1)}; \mathtt{A}'_0, \mathtt{I}_m, \ldots, \mathtt{I}_m) \in \mathcal{S}(n, m)$ is a recursive MDS matrix with $\mathtt{A}'_0 = \mathtt{A}$ for some $\mathtt{A} \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{B}'_t = \mathtt{B}$ for some $\mathtt{B} \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$.*

Proof. Let S be a sparse DSI matrix as given above and $D' = Diag(\mathtt{P}'_0, \mathtt{P}'_1, \ldots, \mathtt{P}'_{n-1}) \in \mathcal{D}(n, m)$. Observe that $S_1 = D'SD'^{-1}$ is also a sparse DSI matrix. We have $S_1[i, j] = D'[i, i]S[i, j]D'^{-1}[j, j] = \mathtt{P}'_i S[i, j]\mathtt{P}'^{-1}_j$ for $0 \leq i, j \leq n-1$ since D' is a block diagonal matrix. We also have $S[i, i-1] = \mathtt{A}_i$ for $1 \leq i \leq n-1$. Now we choose $\mathtt{P}'_i$s such that they satisfy $\mathtt{P}'_{i-1} = \mathtt{P}'_i \mathtt{A}_i$, $1 \leq i \leq n-1$. Therefore we get $S_1[i, i-1] = \mathtt{I}_m$ for $1 \leq i \leq n-1$.

Suppose that $S_1[0, n-1] \in cc(\mathtt{A})$ for some $\mathtt{A} \in \mathcal{N}_{\mathcal{G}}$. Then there exists a matrix $\mathtt{P}_1 \in \mathcal{G} = GL(m, \mathbb{F}_2)$ such that $S_1[0, n-1] = \mathtt{P}_1 \mathtt{A} \mathtt{P}_1^{-1}$. Now consider the matrix

$$S_2 = Diag(\mathtt{P}_1)^{-1} S_1 Diag(\mathtt{P}_1).$$

Observe that we have $S_2[0, n-1] = \mathtt{A}$. Suppose that $S_2[t, t] \in cc_{\mathtt{A}}(\mathtt{B})$ for some $\mathtt{B} \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. Then there exists $\mathtt{P}_2 \in \mathcal{C}_{\mathcal{G}}(\mathtt{A})$ such that $S_2[t, t] = \mathtt{P}_2 \mathtt{B} \mathtt{P}_2^{-1}$. Note that $\mathtt{P}_2^{-1} S_2[0, n-1]\mathtt{P}_2 = \mathtt{P}_2^{-1}\mathtt{A}\mathtt{P}_2 = \mathtt{A}$ since $\mathtt{P}_2 \in \mathcal{C}_{\mathcal{G}}(\mathtt{A})$. Now consider $D = Diag(\mathtt{P}_1\mathtt{P}_2)^{-1}D'$, and it is easy to verify that $S' = DSD^{-1}$ is in the required form. By Lemma 7 we can see that the matrix S' is recursive MDS. □

Remark 5. The LFSR associated with the companion matrix L in Definition 8 is known as Fibonacci LFSR. The state transition matrix of a word-oriented Fibonacci LFSR is of the form given by L. Another well known type of LFSR is Galois LFSR whose state transition matrix is of the form $(L^T)^{-1}$. In [ABMP11] Ring LFSRs are introduced as a generalization. The state transition matrix of a word-oriented Ring LFSR can be given by (see [ABMP11, Def. 3.7])

$$A = \begin{bmatrix} & \mathtt{I}_m & & (*) & \\ & & \ddots & & \\ & (*) & & \ddots & \\ & & & & \mathtt{I}_m \\ \mathtt{I}_m & & & & \end{bmatrix} \tag{2}$$

The above matrix is closely related to the restricted version of the sparse DSI matrices obtained in Theorem 6. So we can see that the sparse DSI matrices are closely related to the word-oriented Ring LFSRs. There have been some works on Ring LFSRs, so an interesting problem is to develop a theory for sparse DSI matrices that yield MDS matrices.

We now present our experimental results. We only get n-MDS sparse DSI matrices of order $n = 4$ over $GL(4, \mathbb{F}_2)$, and for $n = 5, 6, 7, 8$ there is no such matrix. In our search, we first consider $\mathtt{A}_0 = \mathtt{A}(\neq \mathtt{I}_4) \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{B}_0 \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. In the case when $\mathtt{A}_0 = \mathtt{I}_4$, we consider $\mathtt{B}_0 = \mathtt{A} \in \mathcal{N}_{\mathcal{G}}$ and $\mathtt{B}_1 \in \mathcal{N}_{\mathcal{G}}^{\mathtt{A}}$. In this way, we get 236 distinct matrices up to diagonal similarity, and we denote it by $\mathcal{S}^r(4, 4)$. Now we extend it by considering matrices of the form $S' = Diag(\mathtt{P})^{-1} S Diag(\mathtt{P})$ for $S \in \mathcal{S}^r(4, 4)$ and $\mathtt{P} \in GL(4, \mathbb{F}_2)$, and we denote the extended set by $\mathcal{S}^{re}(4, 4)$. In this way, we get $|\mathcal{S}^{re}(4, 4)| = 483,840$ distinct matrices.

Observe that any matrix S' in $\mathcal{S}(4,4)$ is of the form $S' = D^{-1}SD$ for some $S \in \mathcal{S}^{re}(4,4)$ and $D = Diag(\mathtt{I}_4, \mathtt{P}_1, \mathtt{P}_2, \mathtt{P}_3)$, where $\mathtt{P}_1, \mathtt{P}_2, \mathtt{P}_3 \in GL(4, \mathbb{F}_2)$. So we have

$$|\mathcal{S}(4,4)| = |\mathcal{S}^{re}(4,4)| \cdot |GL(4,\mathbb{F}_2)|^3.$$

Also note that there is no involutory 4-MDS sparse DSI matrix in $\mathcal{S}(4,4)$. Now we state our search results.

Theorem 7. *There is no n-MDS sparse DSI matrix of order n over $GL(4,\mathbb{F}_2)$ for $n \in \{5,6,7,8\}$. Also, there is no involutory 4-MDS sparse DSI matrix of order $n = 4$ over $GL(4,\mathbb{F}_2)$.*

In the appendix we present a base set of sparse DSI matrices in $\mathcal{S}^{re}(4,4)$ with the least cost (according to the formula in Table 2) from which we can generate all the sparse DSI matrices with the same cost.

3.5 Recursive MDS Matrices from Sparse DSI Matrices over Finite Fields

The sparse DSI matrices were introduced in [TTKS18]. The authors have provided n-MDS sparse DSI matrices over $\mathbb{F}_{2^m}$ (having low cost) for some parameter values. But they have not provided matrices for many parameter values. Since these matrices have low fixed cost, it is of importance to see whether such matrices exist or not. In this section we discuss many of the issues raised in [TTKS18, Section 7.2].

Throughout this subsection, we assume that $n \geq 2$ and $k = \lfloor \frac{n+1}{2} \rfloor$. We denote the identity matrix in $\mathcal{M}(n,\mathbb{F}_q)$ by I_n. Let $\mathcal{D}(n,\mathbb{F}_q)$ denote the set of nonsingular $n \times n$ diagonal matrices over $\mathbb{F}_q$.

A DSI matrix S of order n over $\mathbb{F}_q$ is given by

$$S = DSI(b_0, b_1, \ldots, b_{n-1}; a_0, a_1, \ldots, a_{n-1}), \tag{3}$$

where $a_i, b_j \in \mathbb{F}_q$ with $a_i \neq 0 \ \forall \ i, 0 \leq i < n$, and $b_j = 0$ for some $j, 0 \leq j < n$, (see Definition 9). Since $b_j = 0$ for some j, the determinant of S is equal to

$$det(S) = \textstyle\prod_{i=0}^{n-1} a_i.$$

The matrix S is nonsingular since $a_i \neq 0, \forall\, i$. Let R_n be the $n \times n$ rotation matrix given by

$$R_n = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \tag{4}$$

and we denote the inverse of R_n by L_n. Observe that $R_n^T = L_n$. We have the following similarity relation over diagonal matrices.

Lemma 15. *Let $D = Diag(d_0, d_1, \ldots, d_{n-1})$ be a diagonal matrix of order n over $\mathbb{F}_q$. Then we have*

$$L_n D R_n = Diag(d_1, d_2, \ldots, d_{n-1}, d_0) \tag{5}$$

Observe that the DSI matrix S in (3) satisfies

$$S = B + AR_n,$$

where $A = Diag(a_0, a_1, \ldots, a_{n-1})$ and $B = Diag(b_0, b_1, \ldots, b_{n-1})$. Now consider the matrix $S' = L_n S R_n$, where S is the DSI matrix mentioned in (3). Then by (5) we have

$$S' = L_n(B + AR_n)R_n = L_nBR_n + (L_nAR_n)R_n = B' + A'R_n,$$

where $A' = Diag(a_1, a_2, \ldots, a_{n-1}, a_0)$ and $B' = Diag(b_1, b_2, \ldots, b_{n-1}, b_0)$. Therefore we have the following result.

Corollary 1. *The DSI matrix $S = DSI(b_0, b_1, \ldots, b_{n-1}; a_0, a_1, \ldots, a_{n-1})$ and its shifted version $S' = DSI(b_1, b_2, \ldots, b_{n-1}, b_0; a_1, a_2, \ldots, a_{n-1}, a_0)$ are permutation similar.*

A DSI matrix $S = DSI(b_0, b_1, \ldots, b_{n-1}; a_0, a_1, \ldots, a_{n-1})$ of order n over $\mathbb{F}_q$ is said to be sparse or simply sparse DSI if $b_i \in \mathbb{F}_q^*$ for i even and 0 otherwise (see Definition 10). So we denote the matrix S by

$$S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a_0, a_1, \ldots, a_{n-1}).$$

Remark 6. For n odd, the definition in [TTKS18] is slightly different from our definition of sparse DSI matrix, but both the matrices are permutation similar. In fact, for n odd, the matrix $L_n^2 S R_n^2$ is in the form defined in [TTKS18, Definition 6] (see also Remark 7).

Let $\mathcal{S}(n, \mathbb{F}_q)$ denote the set of all n-MDS sparse DSI matrices of order n over $\mathbb{F}_q$. From Lemmas 7 and 9 we have the following result for the case of sparse DSI matrices over $\mathbb{F}_q$.

Lemma 16. *If two sparse DSI matrices S and S' over $\mathbb{F}_q$ are diagonal/permutation similar then S is r-MDS if and only if S' is r-MDS.*

With a similar argument as in the proof of Theorem 6 we get the following result in the case of sparse DSI matrices over $\mathbb{F}_q$. For completeness, we present a proof.

Theorem 8. *Let $(a_0, a_1, \ldots, a_{n-1})$ and $(a'_0, a'_1, \ldots, a'_{n-1})$ be two tuples in $(\mathbb{F}_q^*)^n$ such that $a = \prod_{i=0}^{n-1} a_i = \prod_{i=0}^{n-1} a'_i$ for some $a \in \mathbb{F}_q^*$. Then, for any k-tuple $(b_0, b_2, \ldots, b_{2(k-1)}) \in (\mathbb{F}_q^*)^k$, the sparse DSI matrices $S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a_0, a_1, \ldots, a_{n-1})$ and $S' = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a'_0, a'_1, \ldots, a'_{n-1})$ are diagonal similar. In particular, S is diagonal similar to $S'' = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a, 1, \ldots, 1)$. Moreover, we have S is r-MDS if and only if S' (S'') is r-MDS.*

Proof. Let $d_0 = 1$ and $d_i = a'_i a_i^{-1} d_{i-1}$ for $1 \le i \le n-1$. Since $a = \prod a_i = \prod a'_i$, we can see that $S = D^{-1} S' D$, where $D = Diag(d_0, \ldots, d_{n-1})$. By Lemma 16 we get the required result. □

Lemma 17. *Suppose that $S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a, 1, \ldots, 1)$ for some k-tuple $(b_0, b_2, \ldots, b_{2(k-1)}) \in (\mathbb{F}_q^*)^k$ and $a \in \mathbb{F}_q^*$. Then, for any $c \in \mathbb{F}_q^*$, the matrix S is r-MDS if and only if $S' = SpDSI(cb_0, cb_2, \ldots, cb_{2(k-1)}; c^n a, 1, \ldots, 1)$ is r-MDS.*

Proof. Observe that the matrix cS is also sparse DSI and by Theorem 8 we can see that cS is diagonal similar to S'. By Lemma 16 we get the required result. □

We now discuss further reduction by restricting the choices for the element a. Let α be a generator of the cyclic group $\mathbb{F}_q^*$ and let $a = \alpha^i$ for some $0 \le i < (q-1)$. Let $n = 2^\ell t$, where t is odd. Suppose that $i = jt + s$ for some s, $0 \le s < t$. Also note that there always exists a 2^ℓth root of α, say β, in $\mathbb{F}_q^*$. So we have $a = \alpha^i = \beta^{jn}\alpha^s$. Observe that for $c = \beta^{-j}$, the matrix S' in Lemma 17 is given by

$$S' = SpDSI(cb_0, cb_2, \ldots, cb_{2(k-1)}; \alpha^s, 1, \ldots, 1),\ 0 \le s < t.$$

For simplicity, the sparse DSI matrix $S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a, 1, \ldots, 1)$ is denoted by

$$S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a). \tag{6}$$

Let $\hat{\mathcal{S}}(n, \mathbb{F}_q)$ denote the set of all n-MDS sparse DSI matrices over $\mathbb{F}_q$ of the form given in (6) with $a = \alpha^s,\ 0 \leq s < t$, where $n = 2^\ell t$ with t odd and α is a generator of $\mathbb{F}_q^*$. From the discussion above, we can see that any matrix in $\mathcal{S}(n, \mathbb{F}_q)$ can be obtained from a matrix in $\hat{\mathcal{S}}(n, \mathbb{F}_q)$ with suitable transformations given in Lemma 17 and Theorem 8. Let $\hat{\mathcal{B}}(n, \mathbb{F}_q)$ be the set of ordered k-tuples given by

$$\hat{\mathcal{B}}(n, \mathbb{F}_q) = \{(b_0, b_2, \ldots, b_{2(k-1)}) : SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a) \in \hat{\mathcal{S}}(n, \mathbb{F}_q)\}.$$

Similarly, the set of ordered k-tuples $(b_0, b_2, \ldots, b_{2(k-1)})$ appearing in the n-MDS sparse DSI matrices from $\mathcal{S}(n, \mathbb{F}_q)$ is denoted by $\mathcal{B}(n, \mathbb{F}_q)$. From the discussion above we can see the following result.

Lemma 18. *The sets satisfy $\hat{\mathcal{B}}(n, \mathbb{F}_q) \subseteq \mathcal{B}(n, \mathbb{F}_q)$. Moreover, each tuple in $\mathcal{B}(n, \mathbb{F}_q)$ is a constant multiplier of some tuple in $\hat{\mathcal{B}}(n, \mathbb{F}_q)$.*

We now provide some equivalent classes over $\hat{\mathcal{S}}(n, \mathbb{F}_q)$. For this purpose we consider the following permutation matrix

$$J_n = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & \ldots & 1 & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & 1 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \end{pmatrix}.$$

Observe that $J_n^{-1} = J_n$. Let R_n be the matrix given in (4) and L_n be the inverse of R_n. Note that $R_n^T = L_n$ and $J_n R_n J_n = L_n$.

Lemma 19. *If the sparse DSI matrix $S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a)$ is in $\hat{\mathcal{S}}(n, \mathbb{F}_q)$ then the sparse DSI matrix $S' = SpDSI(b_{2(k-1)}, \ldots, b_2, b_0; a)$ is also in $\hat{\mathcal{S}}(n, \mathbb{F}_q)$. Moreover, if $(b_0, b_2, \ldots, b_{2(k-1)}) \in \hat{\mathcal{B}}(n, \mathbb{F}_q)$ then $(b_{2(k-1)}, \ldots, b_2, b_0) \in \hat{\mathcal{B}}(n, \mathbb{F}_q)$.*

Proof. Let $D = Diag(d_0, d_1, \ldots, d_{n-1})$ be a diagonal matrix. It is easy to see that

$$J_n D J_n = Diag(d_{n-1}, \ldots, d_1, d_0). \tag{7}$$

We have $S = B + AR_n$, where $B = Diag(b_0, b_1, b_2, \ldots, b_{n-1})$ with $b_i = 0$ for i odd and $A = Diag(a, 1, \ldots, 1)$. Suppose that n is even. Then consider the matrix $S_1 = L_n J_n S J_n R_n$. Now we can see that

$$S_1 = L_n J_n (B + AR_n) J_n R_n = L_n (J_n B J_n) R_n + L_n (J_n A J_n)$$

Moreover,

$$S_1^T = L_n (J_n B J_n) R_n + (J_n A J_n) R_n.$$

From (5) and (7) and by a careful observation we can see that

$$S_1^T = SpDSI(b_{2(k-1)}, \ldots, b_2, b_0; 1, \ldots, 1, a).$$

Then by Lemma 16 and Theorem 8 we get the required result. In the case where n is odd, we consider $S_1 = J_n S J_n$. By a careful observation, we can see that $S' = S_1^T$. Hence the result. □

Lemma 20. *Let $n \geq 2$ be even. If the sparse DSI matrix $S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a)$ is in $\hat{\mathcal{S}}(n, \mathbb{F}_q)$ then the sparse DSI matrix $S' = SpDSI(b_2, \ldots, b_{2(k-1)}, b_0; a)$ is also in $\hat{\mathcal{S}}(n, \mathbb{F}_q)$. Moreover, if $(b_0, b_2, \ldots, b_{2(k-1)}) \in \hat{\mathcal{B}}(n, \mathbb{F}_q)$ then $(b_2, \ldots, b_{2(k-1)}, b_0) \in \hat{\mathcal{B}}(n, \mathbb{F}_q)$.*

Proof. Consider the matrix $S_1 = L_n^2 S R_n^2$. Clearly, we have

$$S_1 = (L_n^2 B R_n^2) + (L_n^2 A R_n^2) R_n.$$

By a careful observation we can see that $S_1 = SpDSI(b_2, \ldots, b_{2(k-1)}, b_0; 1, \ldots, 1, a, 1)$. By Theorem 8, we can see that S' and S_1 are diagonal similar, and hence the result. □

Remark 7. The above result is valid for even values of n. If n is odd, we have the first and the last entries are nonzero in the diagonal and zeros appear alternatively. Any rotation of the elements in the diagonal violates this condition. However, we can see that by Theorem 8 and Corollary 1 all those matrices are also n-MDS if the matrix S is n-MDS.

Remark 8. In the case where $n = 2^\ell$ we must have $a = 1$ and the elements of $\hat{\mathcal{S}}(n, \mathbb{F}_q)$ are of the form $S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; 1)$. Observe that the transpose of S is in the form of state transition matrix of a Ring LFSR over $\mathbb{F}_q$ (see (2)).

From Lemmas 19 and 20 we have the following result.

Corollary 2. *Suppose that n is even. If $(b_0, b_2, \ldots, b_{2(k-1)}) \in \hat{\mathcal{B}}(n, \mathbb{F}_q)$ then the ordered tuples $(b_j, b_{j+2}, \ldots, b_{j+2(k-1)})$ and $(b_{j+2(k-1)}, b_{j+2(k-2)}, \ldots, b_{j+2}, b_j)$ are also in $\hat{\mathcal{B}}(n, \mathbb{F}_q)$ for j even and $0 \le j \le n-1$, where the indices are taken modulo n.*

We now define an ordering on the elements b_j so that we can consider only one choice among the $2n$ (or 2) permutations of the tuple $(b_0, b_2, \ldots, b_{2(k-1)})$ depending on n is even or odd (see Corollary 2 and Lemma 19). Suppose that the elements of the finite field $\mathbb{F}_q$, $q = 2^m$, are represented with the polynomial basis. We can order the elements according to their value in integer representation, i.e., for an element $a = c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1}$, its integer value representation is given by $int(a) = c_0 + c_1 2 + \cdots + c_{m-1}2^{m-1}$. Then for $a, b \in \mathbb{F}_q$, we say $a \le b$ if $int(a) \le int(b)$. If n is even then define

$$\begin{aligned}\mathcal{S}^r(n, \mathbb{F}_q) = \{&S : S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a) \in \hat{\mathcal{S}}(n, \mathbb{F}_q) \\ &\text{with } b_0 \le b_{2i} \text{ for } 1 \le i \le (k-1) \text{ and } b_2 \le b_{2(k-1)}\}\end{aligned} \tag{8}$$

and if n is odd then define

$$\mathcal{S}^r(n, \mathbb{F}_q) = \{S : S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a) \in \hat{\mathcal{S}}(n, \mathbb{F}_q) \text{ with } b_0 \le b_{2(k-1)}\} \tag{9}$$

From the above discussion in this subsection, we have the following result.

Theorem 9. *Up to diagonal/permutation similarity, any matrix in $\mathcal{S}(n, \mathbb{F}_q)$ is a constant multiple of a matrix in $\mathcal{S}^r(n, \mathbb{F}_q)$.*

So in order to search for n-MDS sparse DSI matrices over $\mathbb{F}_q$ exhaustively, it is enough to search for n-MDS matrices of the form in $\mathcal{S}^r(n, \mathbb{F}_q)$. We have implemented the search technique for $n \times n$ matrices over $\mathbb{F}_{2^m}$ for $n \in \{4, 5, 6, 7, 8\}$ and $m \in \{4, 5, 6, 7, 8\}$, and $n = 8$ and $m = 9$. To verify whether a matrix S is n-MDS, we recursively check that all the submatrices (of order 1 to $n-1$) of S^n are nonsingular. In the process, if we encounter a submatrix which is singular then we exit permanently, and move on to verify the next candidate. We use the determinants of 2×2 submatrices to check the nonsingularity of 3×3 and 4×4 submatrices. The search results are presented in Table 4. We can see that there is no 8-MDS sparse DSI matrix of order 8 over $\mathbb{F}_{2^8}$.

Next we discuss the implementation costs of the sparse DSI matrices over $\mathbb{F}_q$. Recall that the cost of implementing a single iteration of the sparse DSI matrix

$$S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a_0, a_1, \ldots, a_{n-1})$$

is given by

$$Cost(S) = \sum XOR(a_i) + \sum_{b_j \neq a_{(j+1) \bmod n}} XOR(b_j) + k \cdot m, \tag{10}$$

Table 4: Number of n-MDS sparse DSI matrices in $\mathcal{S}^r(n, \mathbb{F}_q)$

Size	Number of n-MDS sparse DSI matrices of order n					
n	$\mathbb{F}_{2^4}$	$\mathbb{F}_{2^5}$	$\mathbb{F}_{2^6}$	$\mathbb{F}_{2^7}$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{2^9}$
4	28	330	1566	7434	30748	-
5	0	150	35010	1463175	21584460	-
6	0	0	0	10857	927480	-
7	0	0	0	0	112000	-
8	0	0	0	0	0	9

where $k = \lfloor \frac{n+1}{2} \rfloor$. Let $a = det(S) = \prod_{i=0}^{n-1} a_i$. Suppose that $a = \prod_{j \in T} b_j$, where T is a subset of $\{0, 2, \ldots, 2(k-1)\}$. Now consider the sparse DSI matrix

$$S' = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a'_0, a'_1, \ldots, a'_{n-1}),$$

where

$$a'_i = \begin{cases} b_{(i-1) \bmod n} & \text{if } (i-1) \bmod n \in T \\ 1 & \text{otherwise} \end{cases}$$

By Theorem 8, if S is n-MDS then S' is also n-MDS. Observe that the cost of implementing a single iteration of the sparse DSI matrix S' is equal to

$$Cost(S') = \sum_{\text{even } j=0}^{2(k-1)} XOR(b_j) + k \cdot m.$$

It is likely that that the sparse DSI matrices having the least cost are of the form S'. Recall that up to diagonal/permutation similarity any n-MDS sparse DSI matrix is a constant multiple of an n-MDS matrix in $\mathcal{S}^r(n, \mathbb{F}_q)$ (see Theorem 9).

Now consider a sparse DSI matrix $S = SpDSI(b_0, b_2, \ldots, b_{2(k-1)}; a) \in \mathcal{S}^r(n, \mathbb{F}_q)$. By Lemma 17, we can see that cS is diagonal similar to $S'' = SpDSI(cb_0, cb_2, \ldots, cb_{2(k-1)}; c^n a)$. If there exists some subset $T \subset \{0, 2, \ldots, 2(k-1)\}$ of size t such that

$$c^t \prod_{j \in T} b_j = c^n a$$

then we can distribute the determinant $det(S'')$ in a_i's and get a matrix whose cost only depends on cb_j's. We apply this technique for the matrices of order n over $\mathbb{F}_{2^8}$ for $n = 4, 5, 6, 7$. We do not get any better matrix than the matrices [TTKS18, Table 4] for $n = 4, 5, 6$. But we get a 7×7 sparse DSI matrix whose cost is 47, whereas the cost of the matrix provided in [TTKS18, Table 4] is 54. We use the same notation for the finite field $\mathbb{F}_{2^8} = \text{GF}(2^8)/\texttt{0x1c3}$ and XOR counts of the elements as in [TTKS18, Appendix B] to present the matrix: $S = SpDSI(b_0, b_2, b_4, b_6; a_0, a_1, \ldots, a_6)$, where $b_0 = a_1 = \texttt{0xe5}, b_4 = a_5 = \texttt{0x91}$ and $b_2, b_6, a_0, a_2, a_3, a_4, a_6$ are equal to 1. We have $XOR(b_0) = 11$ and $XOR(b_4) = 4$. By fixing a basis, we fix the XOR counts of the field elements. For comparison purpose, we have used the table given in [TTKS18, Appendix B]. It may be possible that there exists a basis of $\mathbb{F}_{2^8}$ over $\mathbb{F}_2$ with which we can get s-XOR(b_0) + s-XOR$(b_4) < 15$. In [BKL16], the authors provided methods to find a basis with which the XOR count of a finite field element is optimal. It is an open problem to find an optimal basis such that $\sum_{c \in E} XOR(c)$ is minimal for a subset E of $\mathbb{F}_q^*$ of size $|E| \geq 2$.

Remark 9. Essentially we need to distribute the determinant $c^n a$ of S'' in a_i's such that $\prod a_i = c^n a$ and it optimizes the cost of the matrix S'' as given in (10). It is not difficult to find an optimal distribution even in this general case, and for $n = 7$ we have not got a better solution than the matrix presented above. So the sparse DSI matrix S presented above is one of the best as per the XOR counts given in [TTKS18, Appendix B].

Remark 10. From each matrix $S \in \mathcal{S}^r(n, \mathbb{F}_q)$, we can generate up to $2n\,(2)$ sparse DSI matrices if n is even (odd), and for each such matrix $S' \in \hat{\mathcal{S}}(n, \mathbb{F}_q)$ generated we get $(q-1)^n$ many distinct sparse DSI matrices in $\mathcal{S}(n, \mathbb{F}_q)$, by taking $D^{-1}S'D$, where D is a nonsingular diagonal matrix over $\mathbb{F}_q$.

4 Conclusion

We have considered circulant, Hadamard, companion and sparse DSI matrices over $GL(4, \mathbb{F}_2)$. We have provided a method with which we are able to exhaustively search for MDS matrices of these types for some parameter choices. We have provided circulant MDS matrices of order 8 which were not known before. We have also established the nonexistence of involutory circulant/cyclic MDS matrices of order $6, 8$. It is well known that there is no companion matrix over fields of even characteristic that yields an involutory MDS matrix. With our method, we have obtained companion matrices over $GL(4, \mathbb{F}_2)$ that yield involutory MDS matrices. We have analyzed the structure of sparse DSI matrices over finite fields, and using this we are able to exhaustively search for sparse DSI matrices that yield MDS matrices for some small parameter values. We are able to obtain a sparse DSI matrix of order 7 over $\mathbb{F}_{2^8}$, which is better than the known ones. We have also established the nonexistence of 8-MDS sparse DSI matrices of order 8 over $\mathbb{F}_{2^8}$. A characterization of recursive MDS companion matrices was given in [GPV17], and they are related to Fibonacci LFSRs. We have discussed a relation between (sparse) DSI matrices and Ring LFSRs. It is an interesting open problem to develop a theory for recursive MDS sparse DSI matrices.

Acknowledgments

The authors would like to thank Jérémy Jean and the anonymous reviewers for their valuable suggestions.

References

[ABMP11] François Arnault, Thierry P. Berger, Marine Minier, and Benjamin Pousse. Revisiting LFSRs for cryptographic applications. *IEEE Trans. Information Theory*, 57(12):8095–8113, 2011.

[AF13] Daniel Augot and Matthieu Finiasz. Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. In *IEEE International Symposium on Information Theory 2013*, pages 1551–1555. IEEE, 2013.

[AF14] Daniel Augot and Matthieu Finiasz. Direct construction of recursive MDS diffusion layers using shortened BCH codes. In *FSE 2014*, volume 8540 of *LNCS*, pages 3–17. Springer, 2014.

[BFI19] Subhadeep Banik, Yuki Funabiki, and Takanori Isobe. More results on shortest linear programs. In *IWSEC 2019*, volume 11689 of *LNCS*, pages 109–128. Springer, 2019.

[BKL16] Christof Beierle, Thorsten Kranz, and Gregor Leander. Lightweight multiplication in $GF(2^n)$ with applications to MDS matrices. In *CRYPTO 2016*, volume 9814 of *LNCS*, pages 625–653. Springer, 2016.

[BR99] M. Blaum and R. M. Roth. On lowest density MDS codes. *IEEE Trans. Information Theory*, 45(1):46–59, 1999.

[CL19] Victor Cauchois and Pierre Loidreau. On circulant involutory MDS matrices. *Des. Codes Cryptogr.*, 87(2-3):249–260, 2019.

[Dae95] Joan Daemen. *Cipher and hash function design strategies based on linear and differential cryptanalysis.* PhD thesis, KU Leuven, 1995.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard.* Information Security and Cryptography. Springer, 2002.

[GPP11] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In *CRYPTO 2011*, volume 6841 of *LNCS*, pages 222–239. Springer, 2011.

[GPV17] Kishan Chand Gupta, Sumit Kumar Pandey, and Ayineedi Venkateswarlu. Towards a general construction of recursive MDS diffusion layers. *Des. Codes Cryptogr.*, 82(1-2):179–195, 2017.

[GPV19] Kishan Chand Gupta, Sumit Kumar Pandey, and Ayineedi Venkateswarlu. Almost involutory recursive MDS diffusion layers. *Des. Codes Cryptogr.*, 87(2-3):609–626, 2019.

[GR14] Kishan Chand Gupta and Indranil Ghosh Ray. On constructions of circulant MDS matrices for lightweight cryptography. In *ISPEC 2014*, volume 8434 of *LNCS*, pages 564–576. Springer, 2014.

[JPST17] Jérémy Jean, Thomas Peyrin, Siang Meng Sim, and Jade Tourteaux. Optimizing implementations of lightweight building blocks. *IACR Trans. Symmetric Cryptol.*, 2017(4):130–168, 2017.

[KLSW17] Thorsten Kranz, Gregor Leander, Ko Stoffelen, and Friedrich Wiemer. Shorter linear straight-line programs for MDS matrices. *IACR Trans. Symmetric Cryptol.*, 2017(4):188–211, 2017.

[Köl19] Lukas Kölsch. XOR-counts and lightweight multiplication with fixed elements in binary finite fields. In *EUROCRYPT 2019*, volume 11476 of *LNCS*, pages 285–312. Springer, 2019.

[KPPY14] Khoongming Khoo, Thomas Peyrin, Axel York Poschmann, and Huihui Yap. FOAM: searching for hardware-optimal SPN structures and components with a fair comparison. In *CHES 2014*, volume 8731 of *LNCS*, pages 433–450. Springer, 2014.

[LS16a] Meicheng Liu and Siang Meng Sim. Lightweight MDS generalized circulant matrices. In *FSE 2016*, volume 9783 of *LNCS*, pages 101–120. Springer, 2016.

[LS16b] Meicheng Liu and Siang Meng Sim. Lightweight MDS generalized circulant matrices. *IACR Cryptology ePrint Archive*: https://eprint.iacr.org/2016/186.pdf, 2016.

[LW16] Yongqiang Li and Mingsheng Wang. On the construction of lightweight circulant involutory MDS matrices. In *FSE 2016*, volume 9783 of *LNCS*, pages 121–139. Springer, 2016.

[MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[Pow11] Philip D. Powell. Calculating Determinants of Block Matrices. *arXiv e-prints*: https://arxiv.org/abs/1112.4379, Dec 2011.

[PSA+18] Meltem Kurt Pehlivanoglu, Muharrem Tolga Sakalli, Sedat Akleylek, Nevcihan Duru, and Vincent Rijmen. Generalisation of Hadamard matrix to generate involutory MDS matrices for lightweight cryptography. *IET Information Security*, 12(4):348–355, 2018.

[SKOP15] Siang Meng Sim, Khoongming Khoo, Frédérique E. Oggier, and Thomas Peyrin. Lightweight MDS involution matrices. In *FSE 2015*, volume 9054 of *LNCS*, pages 471–493. Springer, 2015.

[SSSM17] Sumanta Sarkar, Habeeb Syed, Rajat Sadhukhan, and Debdeep Mukhopadhyay. Lightweight design choices for LED-like block ciphers. In *INDOCRYPT 2017*, volume 10698 of *LNCS*, pages 267–281. Springer, 2017.

[Sta12] Richard P. Stanley. *Enumerative Combinatorics*, volume 1. Cambridge University Press, 2012.

[TP19] Quan Quan Tan and Thomas Peyrin. Improved heuristics for short linear programs. *IACR Cryptology ePrint Archive*: https://eprint.iacr.org/2019/847, 2019.

[TTKS18] Dylan Toh, Jacob Teo, Khoongming Khoo, and Siang Meng Sim. Lightweight MDS serial-type matrices with minimal fixed XOR count. In *AFRICACRYPT 2018*, volume 10831 of *LNCS*, pages 51–71. Springer, 2018.

[WWW12] Shengbao Wu, Mingsheng Wang, and Wenling Wu. Recursive diffusion layers for (lightweight) block ciphers and hash functions. In *SAC 2012*, volume 7707 of *LNCS*, pages 355–371. Springer, 2012.

A Experimental Results : Base Sets with the Least Cost

We denote the cost of an MDS matrix M by $Cost_d(M)$ and $Cost_s(M)$ according to d-XOR and s-XOR metrics respectively, where we use the formulas in Table 2 to compute the cost. Some of the matrices are over the finite field $\mathbb{F}_{2^4}$ in matrix representation. We highlight such matrices with * at the end. We present the elements of $GL(4, \mathbb{F}_2)$ in hexadecimal form as given (1). For each type, we now present base sets of matrices with the least cost. By applying appropriate transformations as discussed in this paper, we get all the matrices with the least cost. For each type, we also provide the number of distinct matrices with the least cost.

Circulant MDS Matrices:

$|\{C \in \mathcal{C}(4,4) : Cost_d(C) = 12 + 3 = 15\}| = 13,824.$

```
[0x8421, 0x8421, 0x1843, 0x29c4]*
[0x4821, 0x4928, 0x9482, 0x6841]
[0x2689, 0x4289, 0x4218, 0x8124]
```

$|\{C \in \mathcal{C}(4,4) : Cost_s(C) = 12 + 3 = 15\}| = 18,432.$

```
[0x8421, 0x8421, 0x1843, 0x29c4]*
[0x8421, 0x8421, 0x3187, 0x4298]*
[0x4821, 0x4928, 0x9482, 0x6841]
```

`[0x2689, 0x4289, 0x4218, 0x8124]`

$|\{C \in \mathcal{C}(5,4) : Cost_d(C) = Cost_s(C) = 16+4 = 20\}| = 8,640.$
`[0x8421, 0x1843, 0x4298, 0x4298, 0x1843]`*
`[0x8421, 0x1846, 0x4238, 0x4238, 0x1846]`*
`[0x8421, 0x4192, 0x2816, 0x2816, 0x4192]`

$|\{C \in \mathcal{C}(6,4) : Cost_d(C) = 20+12 = 32\}| = 24,192.$
`[0x8421, 0x1843, 0xb5a6, 0x1843, 0xc6b9, 0x8421]`*
`[0x8421, 0x2943, 0xc5b6, 0x2943, 0x56a8, 0x8421]`*
`[0x1c28, 0xa914, 0x4285, 0xa914, 0x3ad6, 0x1c28]`
`[0xc328, 0x25c8, 0x91a4, 0x4169, 0x461a, 0x5823]`

$|\{C \in \mathcal{C}(6,4) : Cost_s(C) = 20+10 = 30\}| = 20,736.$
`[0x8421, 0x1843, 0xb5a6, 0x1843, 0xc6b9, 0x8421]`*
`[0x8421, 0x1843, 0x8421, 0xef7d, 0x29c4, 0x29c4]`*
`[0x1843, 0x3187, 0x1843, 0xdefa, 0x4298, 0x4298]`*

$|\{C \in \mathcal{C}(8,4) : Cost_d(C) = 28+20 = 48\}| = 36,864.$
`[0x2c85, 0x4186, 0x14a2, 0x834a, 0x69a8, 0x54b9, 0xce53, 0x4193]`
`[0xb6c9, 0x5842, 0x183e, 0x1e42, 0x8162, 0x9726, 0xc41a, 0x28c5]`

$|\{C \in \mathcal{C}(8,4) : Cost_s(C) = 28+17 = 45\}| = 36,864.$
`[0x1348, 0x4ba8, 0xea6f, 0x7b18, 0x2c9d, 0x2853, 0x1284, 0xac41]`
`[0x1348, 0x3729, 0x1284, 0x512d, 0x2c9d, 0x2853, 0xf8eb, 0xac41]`

Involutory Circulant MDS Matrices:
$|\{C \in \mathcal{C}(4,4) : Cost_d(C) = Cost_s(C) = 12+5 = 17\}| = 4 \cdot 24 = 96.$
`[0x8421, 0x1248, 0x4c32, 0xb521]`

$|\{C \in \mathcal{C}(5,4) : Cost_d(C) = Cost_s(C) = 16+4 = 20\}| = 24.$
`[0x8421, 0x4192, 0x2816, 0x2816, 0x4192]`

Hadamard MDS Matrices:
$|\{H \in \mathcal{H}(4,4) : Cost_d(H) = Cost_s(H) = 12+4 = 16\}| = 6,912.$
`[0x85a1, 0x4812, 0x2485, 0xa124]`

$|\{H \in \mathcal{H}(8,4) : Cost_d(H) = 28+26 = 54 \text{ and } Cost_s(H) = 28+20 = 48\}| = 774,144.$
`[0x8421, 0x1843, 0x3187, 0x6b5c, 0x4298, 0xb5a6, 0xdefa, 0x9c62]`*

Involutory Hadamard MDS Matrices:
$|\{H \in \mathcal{H}(4,4) : Cost_d(H) = 12+6 = 18 \text{ and } Cost_s(H) = 12+5 = 17\}| = 24*24 = 576.$
`[0x8421, 0x1843, 0x29c4, 0x3187]`*

$|\{H \in \mathcal{H}(8,4) : Cost_d(H) = 28+36 = 64\}| = 80,640.$
`[0x9d63, 0x4639, 0x65ad, 0xa7b5, 0x2394, 0x5f7b, 0x1942, 0xf8ce]`*
`[0xd96e, 0x467b, 0x61a8, 0xa3f2, 0x27d3, 0x1b34, 0x5d4f, 0xb8c6]`*
`[0xfb68, 0x465c, 0x63a2, 0xa1df, 0x25fe, 0x3915, 0x7f49, 0x98ca]`*
`[0xd9ba, 0x421f, 0x21f8, 0xe7c6, 0x63e7, 0x1f84, 0x5d9b, 0xf842]`*

$|\{H \in \mathcal{H}(8,4) : Cost_s(H) = 28+25 = 53\}| = 32,256.$
`[0x9d63, 0x4639, 0x65ad, 0xa7b5, 0x2394, 0x5f7b, 0x1942, 0xf8ce]`*

4-**MDS Companion Matrices**:
$|\{L \in \mathcal{L}(4,4) : Cost_d(L) = Cost_s(L) = 12 + 2 = 14\}| = 24$.
`[0x4298, 0x1843, 0x4298, 0x8421]`*

Involutory 4-**MDS Companion Matrices**:
$|\{L \in \mathcal{L}(4,4) : Cost_d(L) = 12 + 6 = 18\}| = 48$.
`[0x1482, 0x234c, 0x1a68, 0x9684]`
`[0x1824, 0x9261, 0x8156, 0x43c2]`

$|\{L \in \mathcal{L}(4,4) : Cost_s(L) = 12 + 5 = 17\}| = 48$.
`[0x8421, 0x2581, 0x32bf, 0x1468]`
`[0x8421, 0x4823, 0x5f1d, 0x1468]`

4-**MDS sparse DSI Matrices**:
$|\{S \in \mathcal{S}^{re}(4,4) : Cost_d(S) = Cost_s(S) = 8 + 2 = 10\}| = 48$.
`[0x8421, 0x1843, 0x4298]`*
`[0x1843, 0x8421, 0x4298]`*