IACR Transactions
ISSN XXXX-XXXX, Vol. 0, No. 0, pp. 1–24. DOI:XXXXXXXX

Lightweight Iterative MDS Matrices: How Small Can We Go?

Shun Li[1,3], Siwei Sun[1,2,5] ✉, Danping Shi[1,2,5], Chaoyun Li[3] and Lei Hu[1,2,5]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
[3] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[4] imec-COSIC, Dept. Electrical Engineering (ESAT), KU Leuven, Leuven 3001, Belgium
[5] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
{lishun,sunsiwei,shidanping,hulei}@iie.ac.cn, chaoyun.li@esat.kuleuven.be

Abstract. As perfect building blocks for the diffusion layers of many symmetric-key primitives, the construction of MDS matrices with lightweight circuits has received much attention from the symmetric-key community. One promising way of realizing low-cost MDS matrices is based on the iterative construction: a low-cost matrix becomes MDS after rising it to a certain power. To be more specific, if A^t is MDS, then one can implement A instead of A^t to achieve the MDS property at the expense of an increased latency with t clock cycles. In this work, we identify the *exact lower bound* of the number of nonzero blocks for a 4×4 block matrix to be potentially iterative-MDS. Subsequently, we show that the *theoretically lightest* 4×4 iterative MDS block matrix (whose entries or blocks are 4×4 binary matrices) with minimal nonzero blocks costs at least 3 XOR gates, and a concrete example achieving the 3-XOR bound is provided. Moreover, we prove that there is no hope for previous constructions (GFS, LFS, DSI, and spares DSI) to beat this bound. Since the circuit latency is another important factor, we also consider the lower bound of the number of iterations for certain iterative MDS matrices. Guided by these bounds and based on the ideas employed to identify them, we explore the design space of lightweight iterative MDS matrices with other dimensions and report on improved results. Whenever we are unable to find better results, we try to determine the bound of the optimal solution. As a result, the optimality of some previous results is proved.

Keywords: Lightweight cryptography · MDS matrix · Iterative constructions · Shortest linear program (SLP) · Latency

1 Introduction

Shannon's confusion and diffusion principle is best manifested in the design of symmetric-key cryptographic primitives. In many cases, the round function of an iterative design is clearly separated into non-linear and linear layers to provide confusion and diffusion effects respectively. In this article, we mainly focus on the construction of linear diffusion layers, whose functionality is to spread the internal dependencies as much as possible.

Optimal diffusion layers can be constructed from the so-called Maximal Distance Separable (MDS) matrices whose branch numbers (first defined in [Dae95]) reach the upper bounds. The Advanced Encryption Standard (AES) [DR02] is one of the most prominent designs employing MDS matrices as their linear layers. By using an MDS

Received: 20XX-XX-XX, Accepted: 20XX-XX-XX, Published: 20XX-XX-XX

matrix, AES enjoys an elegant security reasoning with respect to differential and linear attacks. Moreover, its security strength gets strong enough without consuming a large number of rounds, which is preferable for low-latency applications. Therefore, the search for good MDS matrices is a major endeavor of the community.

In recent years, the attention of the community naturally turns to the construction of lightweight MDS matrices due to the rapid development of pervasive computing. The diversity of the application scenarios creates a tension between several (potentially conflict) design considerations such as security, low latency, small area, low power and low energy, leading to a large volume of research. When an MDS matrix is too luxury to be used in certain resource constrained devices, compromises can be made by employing almost MDS matrices [BBI+15, Ava17], linear layers that can be implemented with several bitwise XORs [BJK+16], or even a permutation of the positions of the input signals [BKL+07, BPP+17]. Typically, this kind of compromises has to be compensated by a large number of rounds, and complicates the security proof significantly.

Related Work. The constructions of lightweight MDS matrices can be divided into two categories: *iterative constructions* and *single-cycle constructions*.

Iterative Constructions. By repeatedly multiplying a non-MDS matrix A t times, one obtains the matrix A^t which may enjoy the MDS property. If A^t is implemented in a serialized approach with t clock cycles, the cost of the implementation in terms of area is determined by A regardless of how complicated A^t is. This approach is first proposed by Guo, Peyrin, and Poschmann, and used to construct the diffusion components of the PHOTON hash function [GPP11] as well as the LED block cipher [GPPR11].

One method to obtain iterative MDS matrices is to exhaust certain search space of A with a predefined form, and test whether A^t is MDS [GPP11, TTKS18, GPV17, WWW12, SSSM17]. Another approach for producing iterative MDS matrices is to construct matrices with the iterative-MDS property directly based on some codes (e.g., shortened BCH codes, Gabidulin codes) [AF14, Ber13, CLM16]. However, this approach mainly focuses on providing new methods for direct constructions, and accounts for a very limited spectrum of iterative-MDS matrices. Moreover, with respect to lightweightness, this approach is inferior.

The main drawback of iterative MDS matrices is that the reduced area footprint comes at the cost of increased delays. In certain low-latency applications, we do not have the luxury to compute an MDS matrix with several clock cycles.

Single-cycle Constructions. For this type of constructions, an MDS matrix is supposed to be implemented as a block of combinatorial logic circuit which can be computed in one clock cycle.

Initial efforts on finding lightweight MDS matrices in this category are started with the investigation on the selection of matrix entries enjoying low area footprints [SKOP15, BKL16, LS16, LW16, LW17, SS16a, SS16b, SS17, JPST17, ZWS18, GLWL16]. Then MDS matrices can be constructed from some special classes of matrices (e.g., circulant, Hadamard, Toeplitz, etc.) with lightweight entries [SKOP15, LS16, SS16b]. Generalizing the matrix entries from finite field elements to general linear transformations leads to considerable improvements [BKL16, LW16]. However, optimizing matrix entries are fundamentally heuristic and only locally sound with respect to the real problem of constructing the most lightweight MDS matrices.

Therefore, there is a trend in the community to optimize globally, viewing the implementation of linear transformations (matrices) as the well-known Shortest Linear straight-line Problem (SLP). With this approach, more accurate estimations of hardware costs and more lightweight (involutory) MDS matrices are obtained recently [KLSW17, LSL+19,

BFI19, TP19, Max19]. Another quite special approach is proposed by Duval and Leurent: instead of looking for an optimized circuit of a given matrix, a space of circuits is examined to find the optimal ones yielding MDS matrices [DL18].

Our Contribution. By viewing previous constructions as general block matrices without any special structure, we observe that the minimum number of nonzero blocks of previous iterative MDS constructions in the domain of 4×4 block matrices is 6. We prove that it is impossible for an iterative MDS matrix to have only 4 or less nonzero blocks. Then, we explore the space of 4×4 block matrices with 5 nonzero blocks whose entries (or blocks) are 4×4 binary matrices, and we find that the lightest iterative MDS matrix in this domain can be implemented with only 3 XOR gates. We further prove that the area of this matrix reaches the global minimum in the domain of all 4×4 block matrices (whose blocks are 4×4 binary matrices) with 5 nonzero blocks. Moreover, theoretical analysis shows that there is no hope for previous constructions (GFS, LFS, DSI, and spares DSI) to beat the 3-XOR bound.

However, the 3-XOR implementation requires 451 clock cycles to complete, which is not desirable for low-latency designs. With this in mind, we identify the *exact lower bound* of the number of iterations of 4×4 iterative MDS matrices with 5 nonzero blocks, which turns out to be 14. Then we provide a concrete iterative MDS matrix achieving this bound, whose implementation costs only 7 XOR gates. Moreover, we also try to determine the lower bounds of the number of iterations of iterative MDS matrices of other types.

Guided by the bounds and based on the ideas employed to obtain them, we explore the design spaces of iterative MDS matrices with other dimensions that are mostly interested in the context of lightweight symmetric-key cryptography. As a result, we improve the state-of-the-art, and a comparison is made with previous results in Table 1.

Table 1: A comparison with previous results, where all costs are recalculated with Boyar's SLP heuristic [BMP13]

Domain	Type	#Nonzero blocks	#XOR gates	Clock cycles	Source
$\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$	Sparse DSI	6	10	4	[TTKS18]
	GFS	6	10	4	[WWW12]
	LFS	7	14	4	[KPPY14]
	LFS	7	13	8	[SSSM17]
	General block	5	3	451	Sect. 3
	General block	5	7	14	Sect. 4
$\mathbf{M}_4(\mathbf{M}_8(\mathbb{F}_2))$	GFS	6	18	4	[WWW12]
	Sparse DSI	6	20	4	[TTKS18]
	LFS	7	32	4	[KPPY14]
	General block	5	6	451	Sect. 3
	General block	5	14	14	Sect. 4
	Sparse DSI	6	18	4	Sect. 4
$\mathbf{M}_5(\mathbf{M}_4(\mathbb{F}_2))$	LFS	9	18	5	[GPP11]
	LFS	9	19	5	[WWW12]
	General block	6	6	981	Sect. 3
	General block	8	15	8	Sect. 4
$\mathbf{M}_5(\mathbf{M}_8(\mathbb{F}_2))$	Sparse DSI	8	31	5	[TTKS18]
	LFS	9	35	5	[WWW12]
	General block	6	12	981	Sect. 3
	Sparse DSI	8	30	5	Sect. 4

Whenever we cannot find better results, we try to prove the optimality of the previous results. For example, we prove that the lower bound of the area of a matrix $A \in$

$\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ with 6 nonzero blocks such that its 4th power is MDS is 10. Also, a similar result is proved for iterative MDS matrices in $\mathbf{M}_4(\mathbf{M}_8(\mathbb{F}_2))$. Moreover, we make all of our code and results publicly available at

https://github.com/siweisun/iterative_mds

Remark. Up to now, we do not know much about the security effect caused by an MDS matrix in word-oriented designs beyond its MDS property. For example, considering a design where the MC operation of AES is replaced by a lighter MDS matrix found in this work, we do not know whether there is any security escalation or degeneration due to the differences of the bit-level representations of the MDS matrices. We review a list of papers [SD18, DR09a, DR09b, DR07, DR06] discussing the interactions between linear and nonlinear layers, and we think the most relevant property of an MDS matrix in an AES-like design beyond its branch number is the so-called related differential [DR09b]. We try to search for related differentials of the new design. However, the algorithm proposed in [DR09b] does not apply since it requires that the entries of the underlying matrix are field elements, while the entries of our matrices are general linear transformations. Using a modified version of the algorithm presented in [DR09b], we also find some related differentials for our matrices, which is similar to the MC operation of AES. However, no concrete security implications can be derived since as far as we know, no cryptanalytic technique which can exploit related differentials is known.

Organization. In Section 2, we give some preliminaries on MDS matrices and their implementation costs in terms of both area and latency. In Section 3, we identify the lightest iterative 4×4 MDS matrix with minimal nonzero blocks by enumerating the representatives of carefully established equivalence classes covering all possibilities. We take the circuit latency into account in Section 4 and explore the space of lightweight iterative MDS matrices of other dimensions with low latencies. Section 5 concludes the paper and proposes several open problems.

2 Preliminaries

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathbf{M}_k(\mathbb{R})$ be the set of all $k \times k$ matrices whose entries are in a ring $\mathbb{R}$. Then, every matrix A in $\mathbf{M}_k(\mathbb{F}_{2^n})$ or $\mathbf{M}_k(\mathbf{M}_n(\mathbb{F}_2))$ can be represented as an $nk \times nk$ binary matrix in $\mathbf{M}_{nk}(\mathbb{F}_2)$, which is called the binary representation of A. Typically, we regard a matrix $A \in \mathbf{M}_k(\mathbf{M}_n(\mathbb{F}_2))$ as a block matrix

$$A = \begin{pmatrix} A_{1,1} & \cdots & A_{1,k} \\ \vdots & \ddots & \vdots \\ A_{k,1} & \cdots & A_{k,k} \end{pmatrix}$$

whose entries or blocks are $n \times n$ binary matrices. The $n \times n$ identity matrix is denoted as I_n, and we may omit the subscript when it can be inferred from the context. Also, we use $\theta_{\mathbb{F}_2^n}(A)$ to denote the number of nonzero $n \times n$ binary blocks of A, that is,

$$\theta_{\mathbb{F}_2^n}(A) = \#\{A_{i,j} \neq 0 : 1 \leq i, j \leq k\}.$$

Definition 1. Given a binary vector $x \in \mathbb{F}_2^{nk}$ which is regarded as the concatenation of k n-bit words. The Hamming weight of x over $\mathbb{F}_2^n$ is defined as the number of non-zero n-bit words of x, and is denoted by $\omega_{\mathbb{F}_2^n}(x)$.

Definition 2 ([Dae95])**.** The branch number of a matrix $A \in \mathbf{M}_k(\mathbf{M}_n(\mathbb{F}_2))$ over $\mathbb{F}_2^n$ is defined as

$$\mathcal{B}_{\mathbb{F}_2^n}(A) = \min_{x \in \mathbb{F}_2^{nk} \setminus \{0\}} \{\omega_{\mathbb{F}_2^n}(x) + \omega_{\mathbb{F}_2^n}(Ax)\}.$$

Definition 3. A matrix $A \in \mathbf{M}_k(\mathbf{M}_n(\mathbb{F}_2))$ is MDS over $\mathbb{F}_2^n$ if and only if $\mathcal{B}_{\mathbb{F}_2^n}(A) = k+1$.

We can use the following lemma to check whether a given matrix is MDS.

Lemma 1 ([BR99, LW16])**.** *A matrix in $\mathbf{M}_k(\mathbf{M}_n(\mathbb{F}_2))$ is MDS over $\mathbb{F}_2^n$ if and only if all its square block sub-matrices (whose entries are $n \times n$ binary matrices) are invertible.*

Lemma 2. *An invertible matrix A is MDS if and only if A^{-1} is MDS.*

Definition 4. Let $A \in \mathbf{M}_k(\mathbf{M}_n(\mathbb{F}_2))$. A is called an iterative MDS matrix with MDS order t, denoted by $ord(A) = t$, if t is the smallest positive integer such that A^t is MDS.

Definition 5 (Characteristic polynomial [Wan03])**.** The characteristic polynomial f of a binary matrix $A \in \mathbf{M}_m(\mathbb{F}_2)$ is defined as $f(x) = |xI + A| \in \mathbb{F}_2[x]$, where $|\cdot|$ is the determinant.

Lemma 3 ([DF04])**.** *If f is a characteristic polynomial of $A \in \mathbf{M}_m(\mathbb{F}_2)$, then $f(A) = 0$.*

An $m \times n$ binary matrix $M = (b_{ij})_{1 \le i \le m, 1 \le j \le n}$ is associated with a linear transformation mapping $(x_1, \cdots, x_n)$ to $(y_1, \cdots, y_m)$:

$$\begin{cases} y_1 &= b_{11}x_1 + \cdots + b_{1n}x_n \\ &\cdots \\ y_m &= b_{m1}x_1 + \cdots + b_{mn}x_n \end{cases}. \tag{1}$$

This linear transformation can be implemented with a certain number of XOR gates. We denote the minimum number of XOR gates required to implement (1) by $\mathcal{C}^{\oplus}(M)$, which can be obtained by solving the well-known Shortest Linear Program (SLP) problem. The SLP problem has been shown to be NP-hard [BMP08]. For small matrices, the exact solution of the SLP problem can be obtained with the SAT-based approach [FS10], while for large matrices, some SLP heuristics [BMP13, RTA18, LSL+19, JFP19] are able to produce fairly good solutions. Finally, we would like to emphasis that unlike some metrics somehow based on simple XOR counts, the notation $\mathcal{C}^{\oplus}(\cdot)$ represents the *global minimum* of the cost in terms of circuit area.

Given an iterative MDS matrix A such that $ord(A) = t$, then the MDS matrix A^t can be implemented in a serial approach requiring $\mathcal{C}^{\oplus}(A)$ XOR gates and t cycles. Also, we can implement A^t directly with $\mathcal{C}^{\oplus}(A^t)$ XOR gates such that it can be computed in one clock cycle. In practice, it may be computationally infeasible to obtain a $\mathcal{C}^{\oplus}(A^t)$-XOR implementation of A^t. In such situation, we can apply certain SLP heuristics to A^t to get some compact implementations.

3 Towards the Lightest Iterative MDS Matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$

In this section, we regard all matrices in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ as 4×4 block matrices whose entries are 4×4 binary matrices (the blocks). We prove that if a matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ is iterative-MDS, then it has at least 5 nonzero blocks. Afterwards, we identify the theoretically smallest iterative-MDS matrix with 5 nonzero blocks in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$.

3.1 Iterative MDS Matrices with 5 Nonzero Blocks

We start by recalling existing iterative constructions over $\mathbf{M}_4(\mathbf{M}_n(\mathbb{F}_2))$, and generalize these constructions into a unified view. The structures of four different types of iterative MDS matrices appearing in previous work are listed in Fig. 1.

According to Fig. 1, the number of nonzero blocks for LFS, GFS, DSI, and sparse DSI matrices are 7, 6, 7, and 6, respectively. At this point, a natural question can be asked: what is the *minimum number* of nonzero blocks of A such that A^t can be MDS for some positive integer t ?

$$\begin{pmatrix} 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ * & * & * & * \end{pmatrix} \quad \begin{pmatrix} 0 & I & 0 & 0 \\ 0 & 0 & * & * \\ 0 & 0 & 0 & I \\ * & * & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} * & 0 & 0 & * \\ * & * & 0 & 0 \\ 0 & * & * & 0 \\ 0 & 0 & * & 0 \end{pmatrix} \quad \begin{pmatrix} * & 0 & 0 & * \\ * & 0 & 0 & 0 \\ 0 & * & * & 0 \\ 0 & 0 & * & 0 \end{pmatrix}$$

(a) LFS (b) GFS (c) DSI (d) Sparse DSI

Figure 1: Types of iterative MDS matrices

Lemma 4. *Let $A \in \mathbf{M}_4(\mathbf{M}_n(\mathbb{F}_2))$ with at most four nonzero blocks (i.e., $\theta_{\mathbb{F}_2^n}(A) \leq 4$). Then A^t is not MDS for any positive integer t.*

Proof. Assume that $A \in \mathbf{M}_4(\mathbf{M}_n(\mathbb{F}_2))$ has only four nonzero blocks. If there are two or more blocks in the same row or same column, then $|A^t| = |A|^t = 0$ for any positive integer t. Therefore, A cannot be iterative-MDS in this case. Let the four nonzero blocks of A be in different rows and different columns. We claim that A^t has only four nonzero blocks for any t, and these nonzero blocks are in different rows and different columns. Therefore, A cannot be iterative-MDS.

For $t = 1$, the claim is obviously fulfilled. We assume that the claim is also fulfilled for $t = s$, that is, A^s has only 4 nonzero blocks which are in different rows and different columns. We investigate what happens to $A^{s+1} = A^s A$. Let $B = A^s$ and assume that the p_i-th column of the i-th row of the block matrix $B = A^s$ is nonzero. That is, $B_{i,p_i} \neq 0$, where $1 \leq i, p_i \leq 4$. Also, we use q_i to denote the column number such that A_{p_i,q_i} is a nonzero block, where $1 \leq i, q_i \leq 4$. The i-th row of A^{s+1} is

$$(\sum_{u=1}^{4} B_{i,u}A_{u,1}, \sum_{u=1}^{4} B_{i,u}A_{u,2}, \sum_{u=1}^{4} B_{i,u}A_{u,3}, \sum_{u=1}^{4} B_{i,u}A_{u,4})$$

or $(B_{i,p_i}A_{p_i,1}, B_{i,p_i}A_{p_i,2}, B_{i,p_i}A_{p_i,3}, B_{i,p_i}A_{p_i,4})$, where only the q_i-th column $B_{i,p_i}A_{p_i,q_i}$ is nonzero. In summary, there is one and only one nonzero block in each row of A^{s+1}, which cannot be MDS. □

According to Lemma 4, an iterative MDS matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ has at least 5 nonzero blocks. Next, we show that the MDS order of an iterative MDS matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ is upper bounded by 65535. Consequently, when testing whether a given matrix A is iterative-MDS, we only need to check the MDS property of the matrices in $\{A^t : 1 \leq t \leq 65535\}$.

Lemma 5. *If $A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ is an iterative MDS matrix, then $ord(A) \leq 65535$.*

Proof. For an arbitrary invertible matrix $A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$, the characteristic polynomial of A is $f(x) = |A + xI_{16}|$. Thus $f(A) = 0$ and $deg(f) = 16$. Let $g(x)$, $h(x)$ and $q(x)$ be three polynomials in $\mathbb{F}_2[x]$ such that $g(x) = h(x) + q(x)f(x)$. Then $g(A) = h(A) + q(A)f(A) = h(A)$, indicating that $A^i = A^j$ if and only if $x^i = x^j \mod f(x)$. We consider the following sequence of polynomials

$$[g_1(x) = x \bmod f(x),\ \ g_2(x) = x^2 \bmod f(x),\ \ \ldots,\ g_{2^{16}}(X) = x^{2^{16}} \bmod f(x)],$$

in which each $g(x)$ can be represented as a polynomial with degree less than 16:

$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_{15} x^{15},$$

where $b_i \in \mathbb{F}_2$. We claim that $f(x)$ is not in the sequences, otherwise $A^k = 0$ for some k, contradicting with the fact that A is invertible. Therefore, there are at most $2^{16} - 1 = 65535$ different polynomials in the sequence, which implies that there must be repetitions in the sequence. Assume $g_i = g_j$ or $x^i = x^j \mod f(x)$ with $1 \leq i < j \leq 65536$. We have $A^i = A^j$ or $A^{j-i+1} = A$, where the largest possible values of $j - i$ is 65535. □

At this point, to find the lightest iterative MDS matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ with five nonzero blocks, we have to enumerate all matrices in

$$\{A^t : A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2)), \theta_{\mathbb{F}_2^4}(A) = 5, \text{ and } 1 \leq t \leq 65535\},$$

which is infeasible. Therefore, reducing the search space is necessary.

3.2 Reducing the Search Space

First of all, for a matrix $A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ with $\theta_{\mathbb{F}_2^4}(A) = 5$ to be iterative-MDS, the placement of the 5 nonzero blocks is not arbitrary.

Lemma 6. *Let A be a 4×4 iteratively-MDS matrix with 5 nonzero blocks. Then we can identify 4 blocks (from the 5 nonzero blocks) such that any two of them are in different rows and different columns (for convenience, we say that the four blocks are row-column separated).*

Proof. We prove by contradiction. If any four nonzero blocks of A are not row-column separated, we have two possible cases. In the first case, there is one row of the 4×4 block matrix A contains no nonzero blocks. Then A cannot be iteratively-MDS since for any positive integer t, A^t contains a row of four zero blocks.

In the second case, each row of A contains at least one nonzero block. Let us assume that there are four nonzero blocks at column j_1, j_2, j_3, and j_4 for row 1, 2, 3, and 4, respectively, and the remaining nonzero block is placed at row i and column j. Then $\{j_1, j_2, j_3, j_4, j\} \neq \{1, 2, 3, 4\}$, otherwise we can identify 4 blocks (from the 5 nonzero blocks) such that any two of them are in different rows and different columns. This indicates that A has one zero column, whose powers cannot be MDS. □

However, we are going to see that having 4 nonzero blocks placed at different rows and columns is not sufficient. Given a matrix $A \in \{A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2)) : \theta_{\mathbb{F}_2^4}(A) = 5\}$ such that 4 nonzero blocks of A are row-column separated, it can be decomposed as $A = B + Z$, where B has 4 nonzero blocks from A which are placed at different rows and different columns, and Z has a single nonzero block from A. For example:

$$\begin{pmatrix} 0 & A_1 & 0 & A_5 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & A_1 & 0 & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & A_5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

For the convenience of discussion, we say that B is the *principal component* of A, and Z is the *minor component* of A. Note that the principal and minor components are only defined for a matrix in $\{A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2)) : \theta_{\mathbb{F}_2^4}(A) = 5\}$ such that 4 nonzero blocks of A are row-column separated, which are the only matrices we care about in what follows. It can be easily verified by enumeration that for a given matrix A that can be decomposed as defined, the decomposition is unique, where the minor component contains the single block at row i and column j of A such that both row i and column j of A contains two nonzero blocks.

Next, we show that for a 4×4 block matrix A with 5 nonzero blocks such that 4 of them are row-column separated to be iterative MDS, the positions of the 4 nonzero blocks of the principal component of A is highly restricted: only 6 out of 24 possibilities of the choices of the positions of the 4 nonzero blocks are allowed, which are listed as follows:

$$\begin{pmatrix} 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \\ * & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & * & 0 & 0 \\ 0 & 0 & 0 & * \\ * & 0 & 0 & 0 \\ 0 & 0 & * & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & * & 0 \\ * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \\ 0 & * & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \\ 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & * \\ * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \\ * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \end{pmatrix}. \quad (2)$$

Let us consider a 4×4 block matrix whose 4 nonzero blocks are placed at row i and column j_i, for $i \in \{1, 2, 3, 4\}$. The positions of the nonzero blocks correspond to a

permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ j_1 & j_2 & j_3 & j_4 \end{pmatrix}$, which can be represented as the product of some disjoint cycles. We use the product of cycles to denote the type of the block matrix. Therefore, there are totally $4! = 24$ different types for all 4×4 matrices with 4 row-column separated nonzero blocks. For example,

$$\begin{pmatrix} * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \end{pmatrix}, \begin{pmatrix} * & 0 & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \\ 0 & * & 0 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \\ * & 0 & 0 & 0 \end{pmatrix}$$

are of type $(1)(2)(3)(4)$, $(1,2)(3,4)$, $(1)(2,3,4)$, and $(1,2,3,4)$, respectively.

Remark. Similarly, we can use the cycle notation π of a permutation to denote a block permutation matrix P_π in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$. For example, if $\pi = (1,2,3,4)$, then

$$P_\pi = \begin{pmatrix} 0 & I_4 & 0 & 0 \\ 0 & 0 & I_4 & 0 \\ 0 & 0 & 0 & I_4 \\ I_4 & 0 & 0 & 0 \end{pmatrix},$$

where the 4×4 identity matrices are placed at row-column coordinates $(1,2)$, $(2,3)$, $(3,4)$, and $(4,1)$. Under this notation, we always have $P_\pi^{-1} = P_{\pi^{-1}}$.

Lemma 7. *$A \in \mathbf{M}_k(\mathbf{M}_n(\mathbb{F}_2))$ is an iterative MDS matrix if and only if PAP^{-1} is an iterative MDS matrix, where P is a block permutation matrix.*

Proof. It comes from $(PAP^{-1})^t = PA^tP^{-1}$ and Lemma 1. □

Lemma 8 ([DF04], Chapter 4.3, Proposition 11)**.** *Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. That is, given the permutations σ, τ as*

$$\sigma = (s_1, s_2, \cdots, s_{d_1})(s_{d_1+1}, \cdots, s_{d_2}) \cdots (s_{d_{m-1}+1}, \cdots, s_{d_m})$$
$$\tau = (t_1, t_2, \cdots, t_{d_1})(t_{d_1+1}, \cdots, t_{d_2}) \cdots (t_{d_{m-1}+1}, \cdots, t_{d_m})$$

in cycle notation, one can find some $\pi \in S_n$ such that $\pi\sigma\pi^{-1} = \tau$.

Lemma 9. *Let A be a 4×4 iterative MDS matrix with 5 nonzero blocks. Then the principal component of A has to be one of the following six types : $(1,2,3,4)$, $(1,3,4,2)$, $(1,4,3,2)$, $(1,4,2,3)$, $(1,3,2,4)$, and $(1,2,4,3)$, which are listed in Equation (2).*

Proof. Let A be a 4×4 iterative MDS matrix with 5 nonzero blocks whose principal component B is of a type other than the six possibilities listed in Lemma 9. Then, we claim that there always exists a block permutation matrix P such that the principal component of PAP^{-1} belongs to one of the following types: $(1)(2)(3)(4)$, $(1)(2)(3,4)$, $(1)(2,3,4)$.

For example, let B (the principal component of A) be of type $(1)(2,3)(4)$. According to Lemma 8, we can find a permutation π, such that $\pi(1)(2,3)(4)\pi^{-1} = (1)(2)(3,4)$. It can be verified that the principal component of $P_\pi A P_\pi^{-1}$ is of type $(1)(2)(3,4)$. However, it can be shown that any power of $P_\pi A P_\pi^{-1}$ whose principal component is of type $(1)(2)(3)(4)$, $(1)(2)(3,4)$, or $(1)(2,3,4)$ is always an upper or lower triangular block matrix (by considering the powers of the block structures induced by the types), which cannot be MDS. Due to Lemma 7, A itself cannot be iterative-MDS. Therefore, the principal component cannot be of type $(1)(2)(3)(4)$, $(1)(2)(3,4)$, or $(1)(2,3,4)$. □

Taking one step further, we can show that to find the lightest iterative MDS matrix in $\{A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2)) : \theta_{\mathbb{F}_2^4}(A) = 5\}$, we only need to consider the matrices whose principal components are of type $(1,2,3,4)$.

Let $A, B \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$, and $B = \tau(A)$, where τ is an invertible transformation such that B is iterative-MDS if and only if A is iterative-MDS and $\mathcal{C}^{\oplus}(A) = \mathcal{C}^{\oplus}(B)$ (τ is cost and iterative-MDS invariant). Then, in the searching process, we only need to check one of A, B and ignore the other. Let P and Q be 4×4 block permutation matrices and M be an arbitrary matrix. Then it is obvious that $\mathcal{C}^{\oplus}(P \cdot M) = \mathcal{C}^{\oplus}(M \cdot Q) = \mathcal{C}^{\oplus}(M)$, where PM can be implemented by renaming the output signals of the implementation of M, and MQ can be implemented by renaming the input signals of the implementation of M. Therefore, the transformation $\tau : A \mapsto PAP^{-1}$ presented in Lemma 7 is cost and MDS-iterative invariant.

Lemma 10. *To find the smallest iterative MDS matrix in* $\{A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2)) : \theta_{\mathbb{F}_2^4}(A) = 5\}$*, we only need to consider the case where the principal components of the matrices are of type* $(1, 2, 3, 4)$.

Proof. We only need to show that for any given iterative MDS matrix A whose principal component is of type (a, b, c, d) (one of the six possibilities shown in Lemma 9), A can be transformed into a matrix of type $(1, 2, 3, 4)$ through a series of cost and iterative-MDS invariant operations.

Let a matrix A be of type (a, b, c, d). According to Lemma 8, there is some permutation π such that $\pi(a, b, c, d)\pi^{-1} = (1, 2, 3, 4)$. Then $P_\pi A P_\pi^{-1}$ is of type $(1, 2, 3, 4)$. □

At this point, the search space is restricted to be the following 12 cases:

$$\begin{pmatrix} 0&*&0&* \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&*&0&0 \\ *&0&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&*&0&* \\ *&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&*&0 \end{pmatrix}, \tag{3}$$

$$\begin{pmatrix} *&*&0&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&0&* \end{pmatrix}, \begin{pmatrix} 0&*&0&0 \\ 0&*&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&0&*&* \\ *&0&0&0 \end{pmatrix}, \tag{4}$$

$$\begin{pmatrix} 0&*&*&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&*&0&0 \end{pmatrix}, \begin{pmatrix} 0&*&0&0 \\ 0&0&*&* \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ *&0&0&* \\ *&0&0&0 \end{pmatrix}. \tag{5}$$

Actually, out of the 12 cases, only two cases need to be considered. Let

$$P = \begin{pmatrix} 0&I&0&0 \\ 0&0&I&0 \\ 0&0&0&I \\ I&0&0&0 \end{pmatrix}, Q = \begin{pmatrix} 0&0&I&0 \\ 0&0&0&I \\ I&0&0&0 \\ 0&I&0&0 \end{pmatrix}.$$

Then we have the following three groups of equations:

$$\begin{pmatrix} 0&*&0&* \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix} = P \begin{pmatrix} 0&*&0&0 \\ *&0&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix} P^{-1} = Q^{-1} \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&*&0&* \\ *&0&0&0 \end{pmatrix} Q = P^{-1} \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&*&0 \end{pmatrix} P, \tag{6}$$

$$\begin{pmatrix} *&*&0&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix} = P^{-1} \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&0&* \end{pmatrix} P = P \begin{pmatrix} 0&*&0&0 \\ 0&*&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix} P^{-1} = Q^{-1} \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&0&*&* \\ *&0&0&0 \end{pmatrix} Q, \tag{7}$$

$$\begin{pmatrix} 0&*&*&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix} = P^{-1} \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ 0&0&0&* \\ *&*&0&0 \end{pmatrix} P = P \begin{pmatrix} 0&*&0&0 \\ 0&0&*&* \\ 0&0&0&* \\ *&0&0&0 \end{pmatrix} P^{-1} = Q^{-1} \begin{pmatrix} 0&*&0&0 \\ 0&0&*&0 \\ *&0&0&* \\ *&0&0&0 \end{pmatrix} Q, \tag{8}$$

indicating that the forms of the matrices in each group listed in (3), (4), and (5) can be transformed to each other via a series of invertible operations preserving the area cost and iterative MDS property. Therefore, only three cases has to be considered. Now, we show the matrices presented in Equation (6) cannot be iterative-MDS. Let $B = \begin{pmatrix} 0&A_1&0&M \\ 0&0&A_2&0 \\ 0&0&0&A_3 \\ A_4&0&0&0 \end{pmatrix}$. Then we have

$$\begin{cases} B_{1,1}^t &= B_{1,4}^{t-1} A_4 \\ B_{1,3}^t &= B_{1,2}^{t-1} A_2 \\ B_{1,2}^t &= B_{1,1}^{t-1} A_1 \end{cases},$$

which implies $B^t_{1,1} = B^{t-2}_{1,1}M + B^{t-4}_{1,1}A_1A_2A_3$. Since $B^1_{1,1} = B^3_{1,1} = 0$, $B^t_{1,1}$ must be zero when t is odd. From $B^t_{1,2} = B^{t-1}_{1,1}A_1$, we have $B^t_{1,2} = 0$ when t is even, which cannot be iterative-MDS. Now, we are only left with two cases:

$$\begin{pmatrix} * & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \\ * & 0 & 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & * & * & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \\ * & 0 & 0 & 0 \end{pmatrix}.$$

We can further give some restrictions on their entries.

Lemma 11. *If* $\begin{pmatrix} M & A_1 & 0 & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix}$ *or* $\begin{pmatrix} 0 & A_1 & M & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix}$ *is an iterative MDS matrix in* $\mathbf{M}_4(\mathbf{M}_n(\mathbb{F}_2))$*, then* A_1*,* A_2*,* A_3*, and* A_4 *are nonsingular.*

Proof. It comes from the fact that $\begin{vmatrix} M & A_1 & 0 & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{vmatrix} = \begin{vmatrix} 0 & A_1 & M & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{vmatrix} = |A_1||A_2||A_3||A_4|$. □

3.3 The Global Minimum

According to the previous discussion, the search space can be formulated as the union of the following two sets

$$\{\begin{pmatrix} M & A_1 & 0 & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix} : A_1, A_2, A_3, \text{ and } A_4 \text{ in } \mathbf{M}_4(\mathbb{F}_2) \text{ are nonsigular}\} \tag{9}$$

and

$$\{\begin{pmatrix} 0 & A_1 & M & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix} : A_1, A_2, A_3, \text{ and } A_4 \text{ in } \mathbf{M}_4(\mathbb{F}_2) \text{ are nonsigular}\}. \tag{10}$$

We start a trail search in the space

$$\{\begin{pmatrix} M & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ P & 0 & 0 & 0 \end{pmatrix} : P \text{ is a permutation matrix}\}, \tag{11}$$

and we find a 3-XOR matrix whose 451st power is MDS:

$$\begin{pmatrix} 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{pmatrix}^{451} = \begin{pmatrix} 0&1&0&0&0&0&0&1&0&0&0&1&1&1&1&1 \\ 0&0&1&0&1&0&1&1&1&0&1&1&1&1&0&1 \\ 0&0&0&1&1&0&1&0&1&1&1&1&1&1&0&0 \\ 1&0&1&0&1&1&0&1&1&1&0&1&0&1&1&0 \\ 1&1&0&1&0&1&0&0&0&0&1&0&0&0&1&1 \\ 1&1&1&1&1&0&0&0&0&1&0&0&0&1&1&1 \\ 0&1&1&0&0&0&0&1&1&0&1&0&1&1&1&1 \\ 1&1&0&0&0&0&1&0&0&0&0&1&1&1&1&0 \\ 1&0&1&1&1&1&0&1&0&1&0&0&0&0&1&0 \\ 0&0&1&1&1&1&1&1&1&0&0&0&0&1&0&0 \\ 1&1&0&1&0&1&1&0&0&0&0&1&1&0&1&0 \\ 1&1&1&1&1&1&0&0&0&0&1&0&0&0&0&1 \\ 1&0&1&1&1&0&1&1&1&1&0&1&0&1&0&0 \\ 0&0&1&0&0&0&1&1&1&1&1&1&1&0&0&0 \\ 1&1&0&1&1&1&0&1&0&1&1&0&0&0&0&1 \\ 1&0&1&0&1&1&1&1&1&1&1&0&0&0&1&0 \end{pmatrix}. \tag{12}$$

It turns out that this matrix is the globally smallest iterative MDS matrix in $\{A^t : A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2)), \theta_{\mathbb{F}_2^4}(A) = 5\}$. We call a row of a binary matrix A *heavy* if it contains two or more 1's, and we define $\zeta(A)$ to be the number of different *heavy rows* of A. For example, if $A = \begin{pmatrix} 1&0&0 \\ 0&1&1 \\ 1&0&1 \end{pmatrix}$, and $B = \begin{pmatrix} 1&0&0 \\ 0&1&1 \\ 0&1&1 \end{pmatrix}$, then $\zeta(A) = 2$ and $\zeta(B) = 1$. Under this notation, obviously, we always have $\mathcal{C}^{\oplus}(M) \geq \zeta(M)$ for any matrix M.

Lemma 12. *For an arbitrary iterative MDS block matrix* A *in* $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ *with* $\theta_{\mathbb{F}_2^4}(A) = 5$*, we have* $\mathcal{C}^{\oplus}(A) \geq 3$.

Proof. We only need to consider the following two cases:

$$A = \begin{pmatrix} M & A_1 & 0 & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix} \text{ or } B = \begin{pmatrix} 0 & A_1 & M & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix}. \tag{13}$$

For brevity, we only show that $\mathcal{C}^{\oplus}(A) \geq 3$, and $\mathcal{C}^{\oplus}(B) \geq 3$ can be proved in a similar way. We prove by contradiction. Assuming that $\mathcal{C}^{\oplus}(A) \leq 2$, we have $\zeta(M|A_1) \leq \zeta(A) \leq \mathcal{C}^{\oplus}(A) \leq 2$. Now, we can discuss case by case according to $\zeta(M|A_1)$:

- $\zeta(M|A_1) = 0$. In this case, we have $M = 0$ since A_1 is nonsingular, which is impossible according to Lemma 4.
- $\zeta(M|A_1) = 1$. In this case, A has the following four possibilities:

$$\begin{cases} \text{Case I} & : & A_2, A_3, A_4 \text{ are permutation matrices} \\ \text{Case II} & : & \zeta(A_4) = 1, \text{ and } A_2, A_3 \text{ are permutation matrices} \\ \text{Case III} & : & \zeta(A_2) = 1, \text{ and } A_3, A_4 \text{ are permutation matrices} \\ \text{Case IV} & : & \zeta(A_3) = 1, \text{ and } A_2, A_4 \text{ are permutation matrices} \end{cases} \tag{14}$$

  We exhaustively search through all matrices that comply with the above four possibilities, and no iterative MDS matrix is found. Note that in the search, we can fix all permutation matrices to be the identity matrix.

- $\zeta(M|A_1) = 2$. In this case, we have $\zeta(A_2) = \zeta(A_3) = \zeta(A_4) = 0$, which implies that A_2, A_3, and A_4 are all permutation matrices. Moreover $\zeta(A_1) \leq 1$. Otherwise the two different rows of $(M|A_1)$ cannot be implemented with only two XOR gates. We exhaustively check all matrices of the forms shown in Equation (13) such that $\zeta(A_1) \leq 1$, and no iterative MDS matrix is found.

□

The 3-XOR matrix shown in Equation (12) is not only the theoretically lightest iterative MDS matrix in $\{A : A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2)), \theta_{\mathbb{F}_2^4}(A) = 5\}$, but also sets a lower bound for all previous constructions listed in Figure 1 with respect to circuit area. Therefore, there is no hope to find an iterative MDS matrices which costs less than 3 XOR gates with previous techniques. A detailed analysis can be found in Appendix A.

Note that the 3-XOR matrix is not guaranteed to be the global minimum without the condition that there are only 5 nonzero blocks in the matrix. Although intuitively it is unlikely that there are smaller iterative MDS matrices, we do not rule out the possibilities. Therefore, try to prove that there are no smaller matrices with more nonzero blocks. However, we only succeed with matrices with 6, 7, and 8 nonzero blocks. The proof involves some enumeration strategies which cannot be done for more nonzero blocks. Here, we only present the proof for the case of 6 nonzero blocks, other cases can be proved similarly.

Lemma 13. *For an arbitrary iterative MDS block matrix A in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ with $\theta_{\mathbb{F}_2^4}(A) = 6$, we have $\mathcal{C}^{\oplus}(A) \geq 3$.*

Proof. See Appendix B. □

4 Lightweight Iterative MDS Matrices with Small Orders

While the matrix obtained in the previous section whose area cost reaches the minimum may be of theoretic interest, to the best of our knowledge, employing this matrix as a diffusion layer and using the 3-XOR implementation is hardly desirable given that it

requires 451 cycles to complete the computation and thus suffers from high latency. In this section, we derive some bounds on the MDS orders of certain iterative MDS matrices, and try to find lightweight iterative MDS matrices with minimal MDS orders. Note that we only consider matrices in $\mathbf{M}_4(\mathbf{M}_n(\mathbb{F}_2))$ and $\mathbf{M}_5(\mathbf{M}_n(\mathbb{F}_2))$ with $n = 4$ or 8. These are arguably the most interested dimensions in the context of lightweight symmetric-key cryptography [BFI19, Max19, TP19, ABB+16, CDL+19, GPPR11, GPP11]. First, we give two useful lemmas.

Lemma 14. *Let a block matrix $M = (A \mid B)$, where A and B are $n \times n$ invertible binary matrices. Then $\mathcal{C}^{\oplus}(M) \geq n$, and $\mathcal{C}^{\oplus}(M) = n$ if and only if A and B are both permutation matrices.*

Proof. Due to the invertibility of A and B, M has n different heavy rows. Since for any SLP program, each XOR can generate at most one heavy row, we have $\mathcal{C}^{\oplus}(M) \geq n$.

If A and B are both permutation matrices, then M has n different rows, each of which contains two 1's. Therefore, M can be implemented with n XOR gates, where each XOR gate corresponds to one row of M, which implies $\mathcal{C}^{\oplus}(M) = n$.

Finally, if $\mathcal{C}^{\oplus}(M) = n$ and A, B are not all permutation matrices, then M has at least one row with more than two 1's. Now, there are only two possibilities. Firstly, this row is the sum of two rows of M, which contradicts to the invertibility of A and B. Secondly, this row is the sum of one row of M and a unite row vector $(0, \cdots, 0, 1, 0, \cdots, 0)$, which implies that there are rows of A or B are the same, again contradicting to the invertibility of A and B. Therefore, A and B must be permutation matrix. □

Lemma 14 implies that if A and B are not all permutation matrices, $\mathcal{C}^{\oplus}(M) \geq n + 1$.

Lemma 15. *If $G = \begin{pmatrix} A & B \\ C & 0 \end{pmatrix} \in \mathbf{M}_2(\mathbf{M}_4(\mathbb{F}_2))$, where A, B, C are invertible matrices and $\mathcal{C}^{\oplus}(G) = 5$, then $\zeta(C) \leq 1$.*

Proof. Since $\mathcal{C}^{\oplus}(G) = 5$ and $\mathcal{C}^{\oplus}(G) \geq \zeta(G)$, we have $\zeta(G) \leq 5$. Also, due to the invertibility of A and B, we have $\zeta(A \mid B) = 4$. For matrix G, $\zeta(G) = \zeta(A \mid B) + \zeta(C)$, which implies that $\zeta(C) = \zeta(G) - \zeta(A \mid B) \leq 5 - 4 = 1$. □

4.1 Lightweight Iterative MDS Matrices in $\mathbf{M}_4(\mathbf{M}_n(\mathbb{F}_2))$

First, we give a lemma lower bounding the MDS orders.

Lemma 16. *If A is an iterative MDS matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ with $\theta_{\mathbb{F}_2^4}(A) = 5$, then the exact lower bound of $ord(A)$ is 14.*

Proof. Without loss of generality, we can assume that the numbers of nonzero blocks of the first row, second row, third row, and fourth row of A are 2, 1, 1, and 1, since other patterns can be put into this form with a series of invertible transformations that is iterative-MDS and MDS-order invariant. It can be easily verified that A^t always has some zero block(s) when t is less than 14. Moreover, we can find a concrete A with $ord(A) = 14$. □

The lightest iterative MDS matrix we find with MDS order 14 costs 7 XOR gates, and it is given in the following equation:

$$\left(\begin{array}{cccc|cccc|cccc|cccc}
0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&1&1&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&1&1&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&1&1&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
\hline
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right)^{14}
=
\left(\begin{array}{cccc|cccc|cccc|cccc}
1&0&0&0&0&0&1&0&0&1&0&1&1&0&0&0\\
1&0&0&1&0&0&0&1&1&0&1&0&0&1&1&0\\
1&0&1&0&0&1&0&0&1&0&1&1&1&1&1&1\\
1&1&0&0&1&0&0&0&0&1&1&1&1&0&1&1\\
\hline
0&1&1&1&0&1&1&1&1&1&0&0&1&0&1&1\\
1&0&1&1&1&1&1&0&1&0&1&0&1&1&0&1\\
0&1&0&1&0&0&1&1&1&0&0&0&0&0&1&1\\
1&0&1&0&1&0&0&0&1&0&0&1&0&1&0&0\\
\hline
1&0&1&1&1&1&1&1&1&0&0&0&1&1&0&0\\
1&1&0&1&1&1&0&1&1&0&0&1&1&0&1&0\\
0&0&1&1&1&0&1&0&1&0&1&0&1&0&0&0\\
0&1&0&0&0&0&0&1&1&1&0&0&1&0&0&1\\
\hline
1&1&0&0&1&1&0&1&1&0&0&0&1&0&0&0\\
1&0&1&0&1&1&1&0&0&1&1&0&0&0&0&1\\
1&0&0&0&1&0&0&1&1&1&1&1&1&0&1&0\\
1&0&0&1&0&1&1&0&1&0&1&1&1&1&0&0
\end{array}\right).$$

Lemma 17. *If A is an iterative MDS matrix in $\mathbf{M}_4(\mathbf{M}_n(\mathbb{F}_2))$ with $\theta_{\mathbb{F}_2^4}(A) = 6$, then the exact lower bound of $ord(A)$ is 4. Moreover, when $ord(A) = 4$, there are only two possibilities for the distribution of the nonzero blocks of A:*

$$\begin{pmatrix} * & 0 & * & 0 \\ 0 & * & 0 & * \\ 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 & * & * & 0 \\ * & 0 & 0 & * \\ 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \end{pmatrix}. \tag{15}$$

Proof. Without loss of generality (similar to the proof of Lemma 16), we can assume that the numbers of nonzero blocks of the first row, second row, third row, and fourth row are in non-increasing order. Then we have two possible distributions of the nonzero blocks for the four rows: 3+1+1+1 or 2+2+1+1, which leads to $4\times4\times3\times2+6\times6\times4\times3 = 96+432 = 528$ possibilities with respect to the positions of the nonzero blocks. It can be easily verified that all the 528 possible structures have some zero blocks when their powers are less than 4, and only the matrices with the structures shown in (15) have no zero blocks in their 4th power. □

Lemma 18. *Let A be an iterative MDS matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ with $\theta_{\mathbb{F}_2^4}(A) = 6$ and $ord(A) = 4$. Then $\mathcal{C}^{\oplus}(A) \geq 10$.*

Proof. We prove by showing that there is no iterative MDS matrix with $\theta_{\mathbb{F}_2^4}(A) = 6$, $ord(A) = 4$, and $\mathcal{C}^{\oplus}(A) \leq 9$. According to Lemma 17, the form of A has only two possibilities. Here we only prove for the first possibility shown in Equation (15), the other case can be proved similarly. Let

$$A = \begin{pmatrix} * & 0 & * & 0 \\ 0 & * & 0 & * \\ 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} A_{1,1} & 0 & A_{1,3} & 0 \\ 0 & A_{2,2} & 0 & A_{2,4} \\ 0 & A_{3,2} & 0 & 0 \\ A_{4,1} & 0 & 0 & 0 \end{pmatrix},$$

which can be decomposed into two disjoint parts

$$A_L = \begin{pmatrix} A_{1,1} & A_{1,3} \\ A_{4,1} & 0 \end{pmatrix} \quad \text{and} \quad A_R = \begin{pmatrix} A_{2,2} & A_{2,4} \\ A_{3,2} & 0 \end{pmatrix}.$$

With this decomposition, we have $\mathcal{C}^{\oplus}(A) = \mathcal{C}^{\oplus}(A_L) + \mathcal{C}^{\oplus}(A_R)$. According to Lemma 15, $\mathcal{C}^{\oplus}(A_L) \geq 4$, and $\mathcal{C}^{\oplus}(A_R) \geq 4$.

If $\mathcal{C}^{\oplus}(A_L) = \mathcal{C}^{\oplus}(A_R) = 4$, then the 6 nonzero blocks are all permutation matrices, which is impossible for A to be iterative-MDS.

If one of $\mathcal{C}^{\oplus}(A_L)$ and $\mathcal{C}^{\oplus}(A_R)$ is 5, say $\mathcal{C}^{\oplus}(A_L) = 4$, and $\mathcal{C}^{\oplus}(A_R) = 5$. We generate all 5-XOR linear programs with only 8 input signals, from which all possible A_R's can be obtained. However, no case leads to iterative MDS matrix with MDS order 4. □

According to Lemma 18, the 10-XOR iterative MDS matrices presented in [TTKS18, WWW12] with MDS order 4 cannot be further improved in terms of area without increasing the MDS orders or the number of nonzero blocks. Hence, we do not make any effort to find any lighter iterative MDS matrices in $\{A \in \mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2)) : \theta_{\mathbb{F}_2^4}(A) = 6 \text{ and } ord(A) = 4\}$.

For matrices in $A \in \mathbf{M}_4(\mathbf{M}_8(\mathbb{F}_2))$, we find an 18-XOR matrix

$$\left(\begin{array}{cccccccc|cccccccc|cccccccc|cccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
\hline
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0
\end{array}\right)$$

whose 4th power:

$$\left(\begin{array}{cccccccc|cccccccc|cccccccc|cccccccc}
1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&1&1&0&0&0&0&1&0&1&1&0&0&0&0&1&0&1&1&1&0&0&0&1&0&0&1&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1\\
\hline
1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&1&0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1\\
\hline
0&1&1&0&0&0&0&0&1&0&1&0&0&0&0&1&0&1&0&1&0&0&1&1&1&0&0&0&0&0&0&0\\
1&0&1&1&0&0&0&0&1&0&1&0&0&0&0&1&1&0&1&0&1&0&0&1&1&1&0&0&0&0&0&0\\
0&0&1&1&1&0&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0&0&1&1&0&0&1&1&0&0&0&0\\
0&0&0&1&1&1&0&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0&0&1&0&0&0&1&1&0&0&0\\
0&0&0&0&1&1&1&0&0&0&0&0&0&0&1&1&0&0&1&0&1&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&0&0&0&1&1&0\\
1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&1&0&1&1&0&0&1&0&0&0&0&0&0&0&1&1\\
1&1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&1\\
\hline
1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1\\
1&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&0&0&0&1\\
0&0&1&1&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0\\
0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0
\end{array}\right)$$

is MDS. This matrix is so far the lightest spares DSI iterative MDS matrix. However, previous results have reported an 18-XOR iterative MDS matrix of type GFS [WWW12]. In fact, the 18-XOR result is optimal in certain sense. With the technique used in proving Lemma 18, we can prove the following Lemma.

Lemma 19. *Let A be an iterative-MDS matrix in $\mathbf{M}_4(\mathbf{M}_8(\mathbb{F}_2))$ with $\theta_{\mathbb{F}_2^8}(A) = 6$ and $ord(A) = 4$. Then $\mathcal{C}^{\oplus}(A) \geq 18$.*

We can make some trade-offs between the area and MDS order. For example, we find a 14-XOR iterative MDS matrix whose MDS order is 14:

$$\left(\begin{array}{cccccccc|cccccccc|cccccccc|cccccccc}
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
\hline
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right)^{14} =$$

$$\left(\begin{array}{cccccccc|cccccccc|cccccccc|cccccccc}
1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&1&0&0&0\\
1&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&1&1&1&1&0&0&0\\
1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&1&0&1&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&1&0&0\\
0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1&1&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&1&0&0&0&0&1&0&1&1&1\\
\hline
0&1&1&1&0&0&0&0&0&1&1&1&0&0&0&0&1&1&0&0&0&0&0&0&1&0&1&1&0&0&0&0\\
1&0&1&1&0&0&0&0&1&1&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&1&0&1&0&0&0&0\\
0&1&0&1&0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&1&1&0&0&0&0&0&1&1&1&0&0&0&0&1&1&0&0&0&0&0&1&0&1&1&1\\
0&0&0&0&1&0&1&1&0&0&0&0&1&1&1&0&0&0&0&1&0&1&0&0&0&0&0&1&1&0&1&1\\
0&0&0&0&0&1&0&1&0&0&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&1&0&1&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0\\
\hline
1&0&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
1&1&0&1&0&0&0&0&1&1&0&1&0&0&0&0&1&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0\\
0&0&1&1&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0\\
0&0&0&0&1&0&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&1&1&0&1&0&0&0&0&1&1&0&1&0&0&0&0&1&0&0&1&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&1&1&0&0&0&0&1&0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&1&1&1&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&1\\
\hline
1&1&0&0&0&0&0&0&1&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&1&0&0&1&0&0&0&0\\
1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&1&1&1&1&0&0&0&0&1&0&1&0&0&0&0&0\\
1&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&1&0&1&1&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&1&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&1&1&1&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&1\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&1&1&1&1&0&0&0&0&1&0&1&0\\
0&0&0&0&1&0&0&1&0&0&0&0&0&1&1&0&0&0&0&1&0&1&1&1&0&0&0&0&1&1&0&0
\end{array}\right).$$

We also find an iterative MDS matrix costing 6 XOR gates, whose MDS order is 451:

$$\left(\begin{array}{cccccccc|cccccccc|cccccccc|cccccccc}
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
\hline
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right)^{451} =$$

$$\begin{pmatrix}
0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&1&1&0&0&0&0&1&0&1&1&0&0&0&0&1&1&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&1&1&0&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&1&0&0&0&0&0&1&1&1&0&0&0&0&1&0&1&1&0&0&0&0&1&1&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&0&0\\
0&0&0&0&0&1&0&1&0&0&0&0&0&1&1&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0\\
\hline
1&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0\\
1&1&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&1&1&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&1&1&1&0&0\\
1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&0&0&0&0\\
0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1\\
0&0&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&1&1\\
0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&1&1&1&1\\
0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&0\\
\hline
1&0&1&1&0&0&0&0&1&0&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0\\
1&1&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&0&0&0\\
1&1&1&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&1&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&1&0&0&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0\\
0&0&0&1&1&1&1&0&0&0&0&0&1&1&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
\hline
1&0&1&1&0&0&0&0&1&0&1&1&0&0&0&0&1&1&0&1&0&0&0&0&1&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&0&0&0\\
1&1&0&1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0\\
1&0&1&0&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&1&0&1&1&0&0&0&0&1&0&1&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&0\\
0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1\\
0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&1&1&1&1&0&0&0&1&0&0&0&0\\
0&0&0&0&1&1&0&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&1\\
0&0&0&0&1&0&1&0&0&0&0&0&1&1&1&1&0&0&0&0&1&1&0&0&0&0&0&0&0&1&0&0
\end{pmatrix}.$$

4.2 Lighter Iterative MDS Matrices in $\mathbf{M}_5(\mathbf{M}_n(\mathbb{F}_2))$

Lemma 20. *If A is an iterative MDS matrix in $\mathbf{M}_5(\mathbf{M}_n(\mathbb{F}_2))$ with $\theta_{\mathbb{F}_2^n}(A) \leq 8$, then $ord(A) \geq 5$.*

Proof. The proof is similar to Lemma 16, Lemma 17, and Lemma 20. □

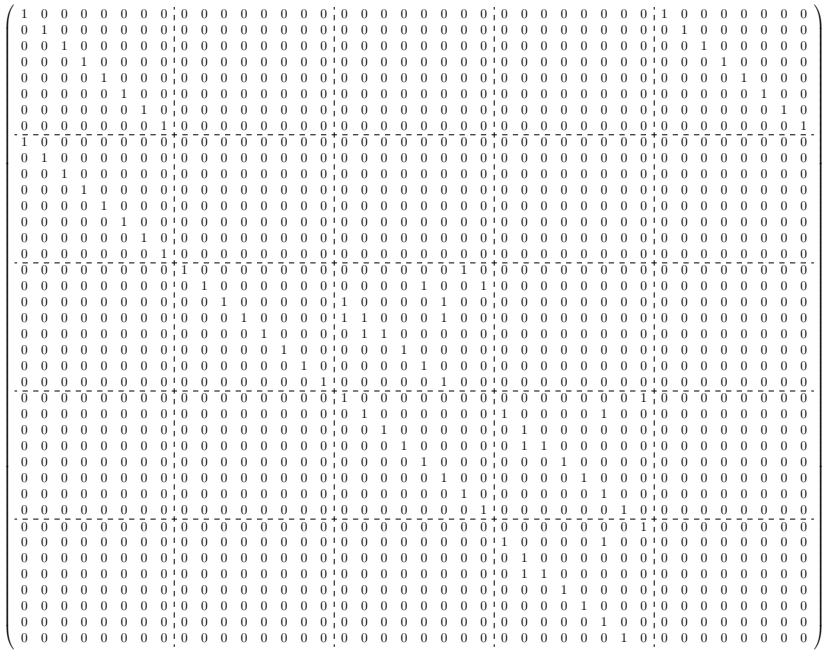
However, we cannot find any lighter iterative MDS matrix in $\mathbf{M}_5(\mathbf{M}_4(\mathbb{F}_2))$ with MDS order 5. It is still possible to find some lighter iterative MDS matrices with large MDS orders. For example, the following is a 6-XOR iterative MDS matrix whose 981st power is MDS:

$$\begin{pmatrix}
1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0\\
\hline
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
\hline
1&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0
\end{pmatrix}^{981}
=
\begin{pmatrix}
0&0&0&1&1&0&0&1&1&0&1&1&1&0&1&0&0&0&0&1\\
0&0&1&1&0&1&1&1&1&1&0&0&1&1&1&1&0&0&1&1\\
1&0&1&0&1&0&0&0&1&1&0&1&0&1&1&1&1&0&1&0\\
0&1&0&0&0&1&0&1&1&1&1&1&1&0&1&1&0&1&0&0\\
\hline
1&0&0&0&1&0&0&0&1&0&0&0&1&1&0&0&1&1&0&1\\
0&1&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&0&0&0\\
0&0&1&0&0&0&1&0&0&1&0&1&1&0&1&0&1&1&0&1\\
0&0&0&1&0&0&0&1&1&0&1&0&0&1&0&1&0&0&1&0\\
\hline
0&0&1&0&1&0&0&0&1&1&0&0&0&0&1&0&0&1&0&0\\
1&0&1&1&0&1&0&0&0&1&0&0&1&1&0&1&0&1&1&0\\
0&1&0&1&1&0&1&0&0&0&1&0&0&1&0&1&1&0&0&1\\
1&0&1&0&0&0&0&1&0&0&0&1&1&0&1&0&1&0&1&0\\
\hline
1&1&1&0&1&0&1&1&0&1&0&1&0&0&1&0&1&0&0&1\\
0&1&1&1&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&1\\
1&0&1&1&1&0&1&0&0&0&0&1&0&1&1&0&0&1&0&0\\
0&1&1&0&1&1&1&1&1&0&1&0&1&0&0&1&1&0&1&0\\
\hline
1&1&1&0&0&1&1&1&0&1&0&1&0&0&1&0&0&1&1&0\\
1&0&0&1&1&0&1&1&1&0&1&0&0&0&0&1&0&0&0&1
\end{pmatrix}.$$

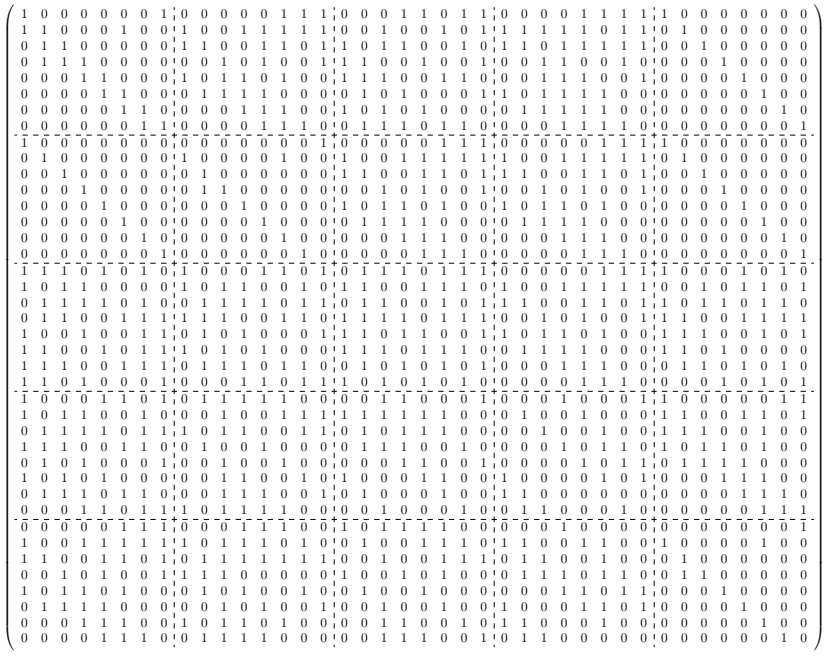
We may make some trade-offs between the MDS order and area. For example, the MDS order of the following 15-XOR iterative MDS matrix is 8:

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0\\
\hline
1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&1&0&0&0&0&1&0&0&0&1&0&0&0&0&0\\
0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&0\\
\hline
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
\hline
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1\\
\hline
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1
\end{pmatrix}^{8}
=
\begin{pmatrix}
0&1&1&0&0&1&1&0&1&1&0&1&1&1&1&0\\
0&0&1&1&0&0&1&1&1&0&1&0&0&1&1&1\\
1&1&0&1&1&1&0&1&0&1&0&1&1&1&1&1\\
1&0&1&0&1&1&1&0&1&1&1&0&1&1&0&1\\
\hline
0&1&0&1&1&0&1&0&0&1&1&0&1&0&0&1\\
1&1&1&0&0&1&0&1&0&0&1&1&1&1&0&1\\
1&1&1&1&0&1&1&0&1&1&0&1&0&0&1&0\\
1&0&0&1&1&1&1&1&1&0&1&0&1&0&0&1\\
\hline
0&1&1&1&1&1&1&0&1&0&0&1&1&0&1&0\\
1&1&0&1&1&0&0&1&1&0&0&1&0&1&1&0\\
1&0&1&0&1&0&1&0&1&1&0&1&0&1&1&0\\
0&1&0&1&1&1&1&0&0&1&0&1&1&0&1&0\\
\hline
0&0&0&1&1&1&0&1&1&1&1&0&1&0&1&1\\
1&1&0&0&1&0&1&0&1&1&0&1&1&0&1&0\\
0&1&1&0&1&1&1&0&1&0&1&0&0&1&0&0\\
0&0&1&1&0&1&1&1&0&1&0&1&1&1&0&0\\
\hline
0&0&0&1&1&0&1&1&1&1&0&0&1&0&1&1\\
1&1&0&0&1&0&0&1&0&1&1&0&1&0&1&0\\
0&1&1&0&1&0&0&0&0&0&1&1&1&0&0&1\\
0&0&1&1&0&1&0&0&1&1&0&1&0&1&1&0
\end{pmatrix}.$$

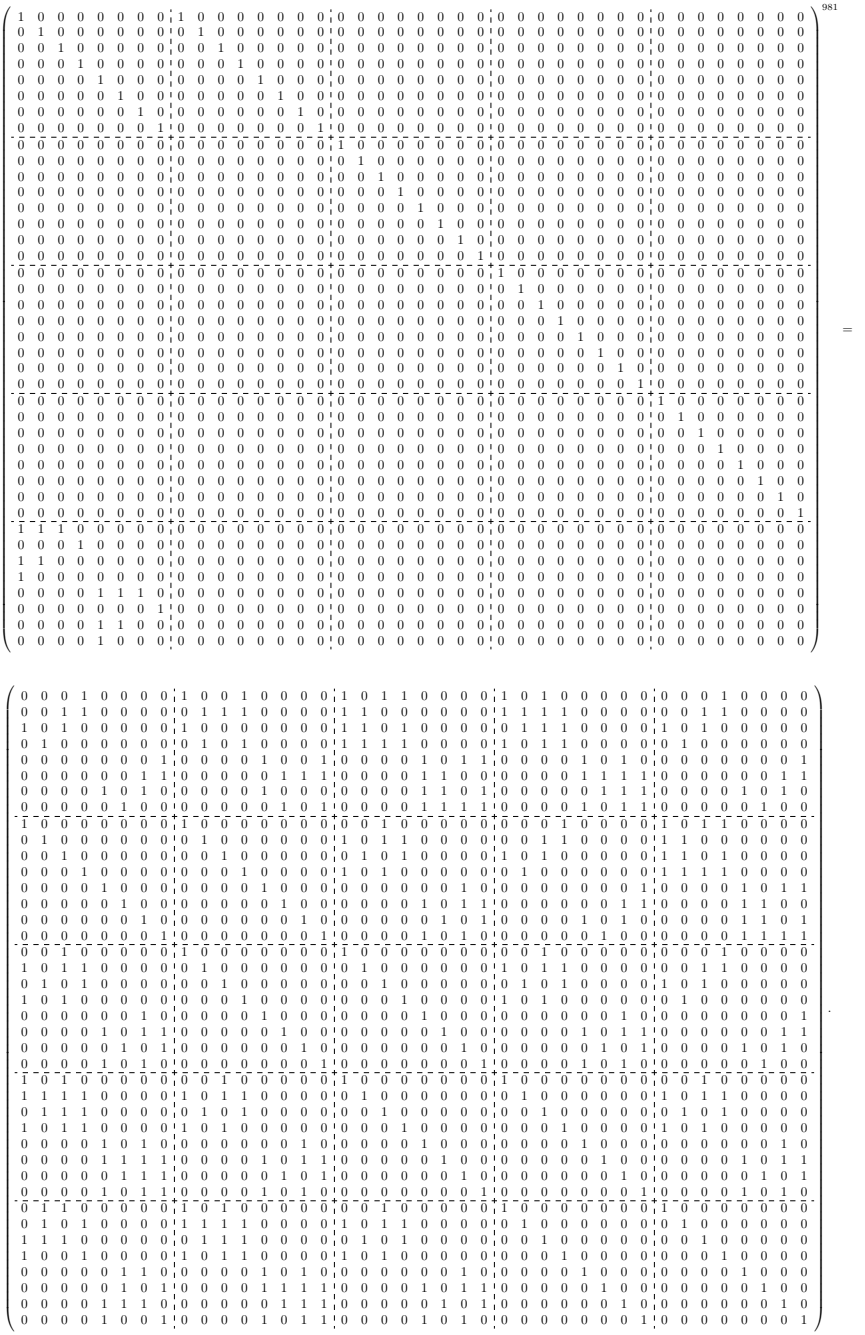
For matrices in $\mathbf{M}_5(\mathbf{M}_8(\mathbb{F}_2))$ We find a 30-XOR matrix (so far the lightest iterative MDS matrix in $\mathbf{M}_5(\mathbf{M}_8(\mathbb{F}_2))$):



whose 5th power



is MDS. If we do not care about the MDS order, the area can be further improved. For example, we find a 12-XOR iterative MDS matrix whose MDS order is 981:



5 Conclusion and Open Problems

In this work, we identify the theoretically lightest iterative MDS matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$ with minimal nonzero blocks, which somehow closes the endeavor of searching for lightweight iterative MDS matrices in this particular domain. Moreover, we report on iterative MDS matrices of various dimensions which are not only lighter than previous results, but also reach their low bounds in terms of latencies. At this point, it is natural to ask some open problems: what is the exact lower bound of the area footprints of the iterative MDS matrices in $\mathbf{M}_4(\mathbf{M}_8(\mathbb{F}_2))$ and $\mathbf{M}_5(\mathbf{M}_n(\mathbb{F}_2))$? Note that it is difficult to solve this problem by using the techniques employed in this work which relies heavily on exhaustive search.

Acknowledgment. The authors thank the anonymous reviewers for many helpful comments. The work is supported by the National Key R&D Program of China (Grant No. 2018YFA0704704), the Chinese Major Program of National Cryptography Development Foundation (Grant No. MMJJ20180102), the National Natural Science Foundation of China (61772519, 61732021, 61802400, 61802399), and the Youth Innovation Promotion Association of Chinese Academy of Sciences. Chaoyun Li is supported by the Research Council KU Leuven: C16/15/058, OT/13/071, and by European Union's Horizon 2020 research and innovation programme under grant agreement No. H2020-MSCA-ITN-2014-643161 ECRYPT-NET.

References

[ABB+16] Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx1, Florian Mendel, Bart Mennink, Nicky Mouha, Qingju Wang, and Kan Yasuda. PRIMATEs v1.02. Submission to CAESAR: Competition for Authenticated Encryption. Security, Applicability, and Robustness, 2016. https://competitions.cr.yp.to/round2/primatesv102.pdf.

[AF14] Daniel Augot and Matthieu Finiasz. Direct construction of recursive MDS diffusion layers using shortened BCH codes. In *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, pages 3–17, 2014.

[Ava17] Roberto Avanzi. The QARMA block cipher family. almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency S-Boxes. *IACR Trans. Symmetric Cryptol.*, 2017(1):4–44, 2017.

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, pages 411–436, 2015.

[Ber13] Thierry P. Berger. Construction of recursive MDS diffusion layers from gabidulin codes. In *Progress in Cryptology - INDOCRYPT 2013 - 14th International Conference on Cryptology in India, Mumbai, India, December 7-10, 2013. Proceedings*, pages 274–285, 2013.

[BFI19] Subhadeep Banik, Yuki Funabiki, and Takanori Isobe. More results on Shortest Linear Programs. In *IWSEC 2019*, 2019. Available at https://eprint.iacr.org/2019/856.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, pages 123–153, 2016.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In *Cryptographic Hardware and*

Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings, pages 450–466, 2007.

[BKL16] Christof Beierle, Thorsten Kranz, and Gregor Leander. Lightweight multiplication in gf(2^n) with applications to MDS matrices. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, pages 625–653, 2016.

[BMP08] Joan Boyar, Philip Matthews, and René Peralta. On the shortest linear straight-line program for computing linear forms. In *Mathematical Foundations of Computer Science 2008, 33rd International Symposium, MFCS 2008, Torun, Poland, August 25-29, 2008, Proceedings*, pages 168–179, 2008.

[BMP13] Joan Boyar, Philip Matthews, and René Peralta. Logic minimization techniques with applications to cryptology. *J. Cryptology*, 26(2):280–312, 2013.

[BPP+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A small present - towards reaching the limit of lightweight encryption. In *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, pages 321–345, 2017.

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

[CDL+19] Anne Canteaut, Sébastien Duval, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Thomas Pornin, and André Schrottenloher. SATURNIN: a suite of lightweight symmetric algorithms for post-quantum security. A Round 1 Candidate of the NIST lightweight crypto standardization process, 2019. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/SATURNIN-spec.pdf.

[CLM16] Victor Cauchois, Pierre Loidreau, and Nabil Merkiche. Direct construction of quasi-involutory recursive-like MDS matrices from 2-cyclic codes. *IACR Trans. Symmetric Cryptol.*, 2016(2):80–98, 2016.

[Dae95] Joan Daemen. Cipher and hash function design strategies based on linear and differential cryptanalysis. Doctoral Dissertation, 1995. https://cs.ru.nl/~joan/papers/JDA_Thesis_1995.pdf.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Wiley Hoboken, 2004.

[DL18] Sébastien Duval and Gaëtan Leurent. MDS matrices with lightweight circuits. *IACR Trans. Symmetric Cryptol.*, 2018(2):48–78, 2018.

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

[DR06] Joan Daemen and Vincent Rijmen. Understanding two-round differentials in AES. In *Security and Cryptography for Networks, 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006, Proceedings*, pages 78–94, 2006.

[DR07] Joan Daemen and Vincent Rijmen. Plateau characteristics. *IET Information Security*, 1(1):11–17, 2007.

[DR09a] Joan Daemen and Vincent Rijmen. New criteria for linear maps in AES-like ciphers. *Cryptography and Communications*, 1(1):47–69, 2009.

[DR09b] Joan Daemen and Vincent Rijmen. New criteria for linear maps in AES-like ciphers. *Cryptography and Communications*, 1(1):47–69, 2009.

[FS10] Carsten Fuhs and Peter Schneider-Kamp. Synthesizing shortest linear straight-line programs over GF(2) using SAT. In *Theory and Applications of Satisfiability Testing - SAT 2010, 13th International Conference, SAT 2010, Edinburgh, UK, July 11-14, 2010. Proceedings*, pages 71–84, 2010.

[GLWL16] Zhiyuan Guo, Renzhang Liu, Wenling Wu, and Dongdai Lin. Direct construction of lightweight rotational-xor MDS diffusion layers. *IACR Cryptology ePrint Archive*, 2016:1036, 2016.

[GPP11] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 222–239, 2011.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED block cipher. In *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, pages 326–341, 2011.

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

[JFP19] Joan, Magnus Gausdal Find, and René Peralta. Small low-depth circuits for cryptographic applications. *Cryptography and Communications*, 11(1):109–127, 2019.

[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.

[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 *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, pages 433–450, 2014.

[LS16] Meicheng Liu and Siang Meng Sim. Lightweight MDS generalized circulant matrices. In *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 101–120, 2016.

[LSL+19] Shun Li, Siwei Sun, Chaoyun Li, Zihao Wei, and Lei Hu. Constructing low-latency involutory MDS matrices with lightweight circuits. *IACR Trans. Symmetric Cryptol.*, 2019(1):84–117, 2019.

[LW16] Yongqiang Li and Mingsheng Wang. On the construction of lightweight circulant involutory MDS matrices. In *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 121–139, 2016.

[LW17] Chaoyun Li and Qingju Wang. Design of lightweight linear diffusion layers from near-MDS matrices. *IACR Trans. Symmetric Cryptol.*, 2017(1):129–155, 2017.

[Max19] Alexander Maximov. AES mixcolumn with 92 XOR gates. Cryptology ePrint Archive, Report 2019/833, 2019. https://eprint.iacr.org/2019/833.

[RTA18] Arash Reyhani-Masoleh, Mostafa M. I. Taha, and Doaa Ashmawy. Smashing the implementation records of AES S-box. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(2):298–336, 2018.

[SD18] Ko Stoffelen and Joan Daemen. Column Parity Mixers. *IACR Trans. Symmetric Cryptol.*, 2018(1):126–159, 2018.

[SKOP15] Siang Meng Sim, Khoongming Khoo, Frédérique E. Oggier, and Thomas Peyrin. Lightweight MDS involution matrices. In *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, pages 471–493, 2015.

[SS16a] Sumanta Sarkar and Siang Meng Sim. A deeper understanding of the XOR count distribution in the context of lightweight cryptography. In *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, pages 167–182, 2016.

[SS16b] Sumanta Sarkar and Habeeb Syed. Lightweight diffusion layer: Importance of Toeplitz matrices. *IACR Trans. Symmetric Cryptol.*, 2016(1):95–113, 2016.

[SS17] Sumanta Sarkar and Habeeb Syed. Analysis of Toeplitz MDS matrices. In *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part II*, pages 3–18, 2017.

[SSSM17] Sumanta Sarkar, Habeeb Syed, Rajat Sadhukhan, and Debdeep Mukhopadhyay. Lightweight design choices for led-like block ciphers. In *Progress in Cryptology - INDOCRYPT 2017 - 18th International Conference on Cryptology in India, Chennai, India, December 10-13, 2017, Proceedings*, pages 267–281, 2017.

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

[TTKS18] Dylan Toh, Jacob Teo, Khoongming Khoo, and Siang Meng Sim. Lightweight MDS serial-type matrices with minimal fixed XOR count. In *Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings*, pages 51–71, 2018.

[Wan03] Zhexian Wan. *Lectures on finite fields and Galois rings*. World Scientific Publishing Company, 2003.

[WWW12] Shengbao Wu, Mingsheng Wang, and Wenling Wu. Recursive diffusion layers for (lightweight) block ciphers and hash functions. In *Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, pages 355–371, 2012.

[ZWS18] Lijing Zhou, Licheng Wang, and Yiru Sun. On efficient constructions of lightweight MDS matrices. *IACR Trans. Symmetric Cryptol.*, 2018(1):180–200, 2018.

A Nonexistence of 2-XOR (Sparse) DSI, LFS, and GFS Iterative MDS matrix in $\mathrm{M}_4(\mathrm{M}_4(\mathbb{F}_2))$

Sparse DSI. Let M be an iterative sparse DSI MDS matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$:

$$M = \begin{pmatrix} B_1 & 0 & 0 & A_1 \\ A_2 & 0 & 0 & 0 \\ 0 & A_3 & B_3 & 0 \\ 0 & 0 & A_4 & 0 \end{pmatrix},$$

where A_i's and B_i's are nonzero. Then $\mathcal{C}^{\oplus}(M) = \mathcal{C}^{\oplus}(U) + \mathcal{C}^{\oplus}(V)$, where

$$U = \begin{pmatrix} B_1 & A_1 \\ A_2 & 0 \end{pmatrix} \text{ and } V = \begin{pmatrix} A_3 & B_3 \\ 0 & A_4 \end{pmatrix}. \tag{16}$$

Since the invertibility of M relies on the invertiblity of A_1, A_2, A_3, and A_4, together with the fact that $B_1 \neq 0$ and $B_3 \neq 0$, we have $\mathcal{C}^{\oplus}(U) \geq 1$ and $\mathcal{C}^{\oplus}(V) \geq 1$, which implies $\mathcal{C}^{\oplus}(M) \geq 2$.

Next, we show that to have $\mathcal{C}^{\oplus}(U) = 1$ and $\mathcal{C}^{\oplus}(V) = 1$ simultaneously is impossible. In this case, A_1, A_2, A_3, A_4 must be permutation matrices. Thus $\mathcal{C}^{\oplus}(U) = \mathcal{C}^{\oplus}(B_1|A_1) = \mathcal{C}^{\oplus}(V) = \mathcal{C}^{\oplus}(A_3|B_3) = 1$, indicating that $\zeta(B_1|A_1) = \zeta(A_3|B_3) = 1$. We exhaust all such matrices and do not find an iterative MDS matrix.

DSI. Let M be an iterative DSI MDS matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$:

$$M = \begin{pmatrix} B_1 & 0 & 0 & A_1 \\ A_2 & B_2 & 0 & 0 \\ 0 & A_3 & B_3 & 0 \\ 0 & 0 & A_4 & 0 \end{pmatrix},$$

where A_1, A_2, A_3, and A_4 are invertible and B_1, B_2, and B_3 are nonzero. It requires at least 3 XOR gates since $\zeta(M) \geq 3$, where the different heavy rows come from $(B_1|A_1)$, $(A_2|B_2)$, and $(A_3|B_3)$.

LFS. The case of LSF matrices can be proved in a similar way as the DSI case.

GFS. Let M be an iterative GSI MDS matrix in $\mathbf{M}_4(\mathbf{M}_4(\mathbb{F}_2))$:

$$M = \begin{pmatrix} 0 & I_4 & 0 & 0 \\ 0 & 0 & A_3 & A_4 \\ 0 & 0 & 0 & I_4 \\ A_1 & A_2 & 0 & 0 \end{pmatrix}.$$

Then $\mathcal{C}^{\oplus}(M) = \mathcal{C}^{\oplus}(U) + \mathcal{C}^{\oplus}(V)$, where

$$U = \begin{pmatrix} 0 & I_4 \\ A_1 & A_2 \end{pmatrix} \text{ and } V = \begin{pmatrix} A_3 & A_4 \\ 0 & I_4 \end{pmatrix}. \tag{17}$$

Similar to the case of sparse DSI, we do not find any iterative MDS matrix such that $\mathcal{C}^{\oplus}(U) \leq 1$ and $\mathcal{C}^{\oplus}(V) \leq 1$.

B Proof of Lemma 13

Proof. We consider $\theta_{\mathbb{F}_2^4}(A_{1,*})$, $\theta_{\mathbb{F}_2^4}(A_{2,*})$, $\theta_{\mathbb{F}_2^4}(A_{3,*})$, and $\theta_{\mathbb{F}_2^4}(A_{4,*})$, where $A_{i,*}$ is the i-th row of A. We can perform elementary row and column operations on A to make $\theta_{\mathbb{F}_2^4}(A_{1,*}) \geq \theta_{\mathbb{F}_2^4}(A_{2,*}) \geq \theta_{\mathbb{F}_2^4}(A_{3,*}) \geq \theta_{\mathbb{F}_2^4}(A_{4,*})$ without changing its cost and iterative-MDS property. Then, we only need to consider the following two cases (the reason is similar to the 5-nonzero-block situation):

$$\begin{cases} \text{Case I} : \theta_{\mathbb{F}_2^4}(A_{1,*}) = 3, \theta_{\mathbb{F}_2^4}(A_{2,*}) = \theta_{\mathbb{F}_2^4}(A_{3,*}) = \theta_{\mathbb{F}_2^4}(A_{4,*}) = 1 \\ \text{Case II} : \theta_{\mathbb{F}_2^4}(A_{1,*}) = \theta_{\mathbb{F}_2^4}(A_{2,*}) = 2, \theta_{\mathbb{F}_2^4}(A_{3,*}) = \theta_{\mathbb{F}_2^4}(A_{4,*}) = 1 \end{cases}$$

For the first case, we only need to consider the following three configurations:

$$A = \begin{pmatrix} M & A_1 & N & 0 \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} M & A_1 & 0 & N \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix}, \text{ or } \begin{pmatrix} 0 & A_1 & M & N \\ 0 & 0 & A_2 & 0 \\ 0 & 0 & 0 & A_3 \\ A_4 & 0 & 0 & 0 \end{pmatrix}.$$

A_1 is non-singular since A is iterative-MDS and non-singular. If $\mathcal{C}^{\oplus}(A) \leq 2$, then A_2, A_3, A_4 are permutation matrices and $\mathcal{C}^{\oplus}(A_1|M|N) \leq 2$. We exhaustively search through all matrices that comply with the above three configurations, and no iterative-MDS matrix is found.

For case II, we have two possible configurations. In the first configuration, two nonzero blocks in $A_{1,*}, A_{2,*}$ are placed at the same column. Up to equivalence, we have only one possibility:

$$A = \begin{pmatrix} 0 & M_1 & M_2 & 0 \\ 0 & M_3 & M_4 & 0 \\ 0 & 0 & 0 & A_1 \\ A_2 & 0 & 0 & 0 \end{pmatrix},$$

where $\mathcal{C}^{\oplus}(A) = \mathcal{C}^{\oplus}(A_1) + \mathcal{C}^{\oplus}(A_2) + \mathcal{C}^{\oplus}\begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix}$. We exhaustively search through all possible 8×8 non-singular matrices $\begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix}$ with XOR-count less than 3, no iterative-MDS matrix is found for A. In the second configuration, two nonzero blocks in $A_{1,*}, A_{2,*}$ have different column coordinates. Then $\mathcal{C}^{\oplus}(A_{1,*}) = \mathcal{C}^{\oplus}(A_{2,*}) = 1$ and $\mathcal{C}^{\oplus}(A_{3,*}) = \mathcal{C}^{\oplus}(A_{4,*}) = 0$. We exhaustively search through all matrices that comply with the above requirement, and no iterative-MDS matrix is found. □