IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2017, No. 4, pp. 169–187. DOI:10.13154/tosc.v2017.i4.169-187

# Direct Construction of Optimal Rotational-XOR Diffusion Primitives

Zhiyuan Guo[1,3,4], Renzhang Liu[2](✉), Si Gao[1,4], Wenling Wu[1,3,4] and Dongdai Lin[2]

[1] TCA Labaratory, State Key Laboratory of Computer Science (SKLCS), Institute of Software, Chinese Academy of Sciences, Beijing, China, gzhyuan@msn.cn,wwl@tca.iscas.ac.cn
[2] State Key Laboratory of Information Security (SKLOIS), Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China, liurenzhang@iie.ac.cn,ddlin@iie.ac.cn
[3] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
[4] University of Chinese Academy of Sciences, Beijing, China

**Abstract.** As a core component of SPN block cipher and hash function, diffusion layer is mainly introduced by matrices built from maximum distance separable (MDS) codes. Up to now, most MDS constructions require to perform an equivalent or even exhaustive search. In this paper, we study the cyclic structure of rotational-XOR diffusion layer, a commonly used diffusion primitive over $(\mathbb{F}_2^b)^n$, which consists of only rotation and XOR operations. First, by providing some novel properties on this class of matrices, we prove the lower bound on the number of rotations for $n \geq 4$, and show the tightness of this bound for $n = 4$. Next, through characterizing the relation among sub-matrices for each possible form, we eliminate all the other non-optimal cases. Finally, we present a direct construction of such MDS matrices, which allows to generate $4 \times 4$ perfect instances for arbitrary $b \geq 4$. Every example contains the fewest possible rotations, so under this strategy, our proposal costs the minimum gate equivalents (resp. cyclic shift instructions) in the hardware (resp. software) implementation. To the best of our knowledge, it is the first time that rotational-XOR MDS diffusion layers have been constructed without any auxiliary search.

**Keywords:** Lightweight Cryptography · MDS Diffusion Layers · Bit-wise Circulant Matrices · Multiple Platforms

## 1 Introduction

As a central part in the substitution-permutation network, diffusion layer is very important for the overall security and efficiency of cryptographic schemes. On the one hand, it plays a role in spreading internal dependencies, which contributes to enhancing the resistance against statistical cryptanalysis. On the other hand, due to the importance of ubiquitous computing and the rapid development of lightweight cryptography, designing diffusion layers with efficient hardware/software implementations has already been a hot research topic [GWG15, SDMO12, SKOP15, LBs+16, SS16].

The quality of a diffusion layer is connected to its branch number [DR02], whose cryptographic significance corresponds to the minimal number of active S-boxes in any two consecutive rounds. From a coding theory perspective, maximum distance separable (MDS) codes are quite good choices for the construction of diffusion layers, as their branch numbers are maximal [MS77]. However, a problem is that using MDS matrix usually comes at the price of a less efficient implementation. Due to Galois field multiplications, hardware implementations will often suffer from an important area requirement, with


Received: 2016-09-01, Revised: 2017-09-01, Accepted: 2017-11-01, Published: 2017-12-15

the result that MDS matrices are sometimes not suitable for the resource-constrained environments, such as RFID systems and sensor networks.

To deal with this dilemma, one common way is to construct lightweight MDS matrices using recursive strategy, which is first adopted in the design of lightweight hash function Photon [GPP11] and block cipher LED [GPPR11]. Its main idea is choosing a linear transformation which is sparse and compact, and composing it several times to obtain an easy-to-implement MDS matrix (also called serial matrix). Such proposal is further generalized in [SDMS12, WWW12], and also connected with coding theory [AF14, Ber13]. Since each entry in a serial matrix is selected with relatively low XOR count [KPPY14], this recursive approach often provides a good way to save hardware area. For a diffusion matrix of order $k$, serial-based implementation computes its nontrivial row (i.e. the last row), and then applies it for $k$ times recursively. As a result, this method inevitably requires more clock cycles, which makes it not suited for round-based or low-latency implementation.

Another trend is constructing lightweight MDS matrices by use of circulant structure [Dav80], which is popular in the design of symmetric-key algorithms [DKR97, DR02]. For hardware implementations, the benefit of a circulant matrix is that all rows are similar (up to a right shift), and we can trivially reuse the multiplication circuit to save silicon area. Namely, it is actually possible for the round-based implementation to compute only one row of a circulant matrix. Therefore, using a circulant matrix gives adequate flexibility to do a trade-off between the area requirement and clock cycle, whereas most of the other matrix types are suitable for either one but not both circumstances.

However, most current constructions of MDS circulant matrices require to perform an equivalent or even exhaustive search [GR14, LW16, LS16]. The time complexity of checking MDS property is unacceptable when the matrix size is large, so those methods are only applicable for relatively small dimensions. One exception is the approach of Augot et al. [AF14], who directly generate MDS matrices using shortened BCH codes (implying that they still need another algorithm in advance to find MDS cyclic codes). Thus an instinctive question is whether we can construct circulant MDS matrices with no auxiliary search. In addition, current lightweight constructions focus mainly on hardware implementation, with little concern on the software performance. Considering an algorithm might be implemented in various platforms, it is an obvious advantage if software performance of the proposed diffusion layer can be improved without loss of hardware efficiency. This paper is devoted to tackle these problems.

**Our contributions.** In this paper, we investigate the construction of rotational-XOR MDS diffusion layer over $(\mathbb{F}_2^b)^n$, which contains only rotation and XOR operations. By providing a series of novel observations on this cyclic structure, we precisely characterize the relation among sub-matrices for each possible perfect form. After eliminating all the other non-optimal cases, we get a direct construction of rotational-XOR MDS linear layers for $n = 4$, which allows to generate $4 \times 4$ MDS instances for arbitrary $b \geq 4$. Compared with block-wise circulant matrices, our bit-wise circulant matrices are more attractive on certain processors, since each rotation can be implemented with a single instruction. As far as we know, it is the first time that rotational-XOR MDS diffusion layers have been directly constructed with no auxiliary search.

**Organization.** In Section 2, we provide some notations and related propositions which are useful for the later proofs. After formally defining a rotational-XOR diffusion layer, we present important observations on this class of matrices in Section 3. We illustrate possible forms of perfect rotational-XOR diffusion layer and check the MDS property for each of them in Section 4. Afterwards, a direct construction of rotational-XOR MDS matrices is deduced in Section 5. We compare the implementation cost in terms of XOR count with the best known results in Section 6. Finally, a brief conclusion is given in Section 7.

## 2 Preliminaries

In this section, we fix basic notations and introduce what branch number is. After giving several useful properties, we formally define a rotational-XOR diffusion layer, which has been widely used in the design of symmetric-key ciphers. Since diffusion layers investigated in the present paper are linear transformations over $(\mathbb{F}_2^b)^n$, we directly use an $n \times n$ matrix with each block size $b \times b$ to represent a linear layer in the subsequent discussions.

### 2.1 Notations

- $|M|$ : Determinant of the matrix $M$.
- $\lll$ : Bit-wise left rotation on $(n \cdot b)$-bit vectors.
- $wt(\boldsymbol{x})$ : Number of nonzero entries of the vector $\boldsymbol{x}$.
- $GL(b, S)$ : Set of all $b \times b$ non-singular matrices with entries in $S$.
- $\boldsymbol{e}_i$ : Standard unit vector, i.e. a binary vector with 1 only at the $i$-th position.

### 2.2 Branch number

Throughout this paper, vectors are represented as columns and subscript index values begin at 1, unless otherwise stated. Assume $\boldsymbol{x} = (\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_n)$ is an $(n \cdot b)$-bit input vector, where $\boldsymbol{x}_i \in \mathbb{F}_2^b$, $1 \le i \le n$. Then the corresponding output of $M$ can be expressed as $M(\boldsymbol{x}) = M \cdot \boldsymbol{x}$. Recall that the diffusion power of $M$ is often quantified by the branch number, an important criterion proposed by Daemen and Rijmen [DR02].

**Definition 1.** The differential branch number of a diffusion layer $M$ is denoted by

$$\mathcal{B}_d(M) = \min_{\boldsymbol{x} \in (\mathbb{F}_2^b)^n, \boldsymbol{x} \neq \boldsymbol{0}} \{wt(\boldsymbol{x}) + wt(M \cdot \boldsymbol{x})\}.$$

Analogously, we can define the linear branch number.

**Definition 2.** The linear branch number of a diffusion layer $M$ is denoted by

$$\mathcal{B}_l(M) = \min_{\boldsymbol{x} \in (\mathbb{F}_2^b)^n, \boldsymbol{x} \neq \boldsymbol{0}} \{wt(\boldsymbol{x}) + wt(M^T \cdot \boldsymbol{x})\},$$

where $M^T$ is the transpose of $M$.

For a diffusion layer acting on $n$ entries, the maximum $\mathcal{B}_d$ and $\mathcal{B}_l$ are both $n+1$ (known as the singleton bound [MS77]). If $\mathcal{B}_d(M) = \mathcal{B}_l(M) = n + 1$, $M$ is called a perfect or MDS diffusion layer. A linear layer has a maximum $\mathcal{B}_d$ if and only if it has a maximum $\mathcal{B}_l$ [DR02], and therefore we omit linear branch number in the sequel.

**Proposition 1.** *Let $M = (M_{i,j})$ and $M' = (M'_{i,j})$, $1 \le i, j \le n$, where $M_{i,j}$ and $M'_{i,j}$ are all $b \times b$ matrices over $\mathbb{F}_2$. If there exists a linear transformation $P \in GL(b, \mathbb{F}_2)$ such that*

$$M'_{i,j} = M_{i,j} \cdot P$$

*for every entry of $M'$, then $M$ and $M'$ are of the same branch number.*

Now suppose $U = [u_1, ..., u_t]$ and $V = [v_1, ..., v_t]$ are two sequences of length $t$, where $1 \le u_1 < \cdots < u_t \le n$, $1 \le v_1 < \cdots < v_t \le n$. We denote the square sub-matrix of $M$ of order $t$ by

$$M(U, V) = (M_{u_j, v_j}, 1 \le j \le t).$$

Thereby the results of [BR99] and [MS77] can be re-described as the following statement.

**Proposition 2.** *Assume $M = (M_{i,j})$, $1 \le i, j \le n$, and the entries of $M$ are $b \times b$ matrices over $\mathbb{F}_2$. $M$ is MDS if and only if its every square sub-matrix of order $t$ is non-singular for $1 \le t \le n$.*

### 2.3 Diffusion layer based on rotations and XORs

In this paper, we consider linear layers over the vector space $(\mathbb{F}_2^b)^n$ constructed by only left-rotation and XOR operations. It is called rotational-XOR diffusion layer and can be formally defined as follows.

**Definition 3.** Let $n$, $b$ be positive integers and $\mathcal{I} \subset \{0, 1, ..., n \cdot b - 1\}$. A rotational-XOR diffusion layer determined by $\mathcal{I}$ over $(\mathbb{F}_2^b)^n$ is denoted by $M_{n,b}^{\mathcal{I}}$, which can be characterized as

$$M_{n,b}^{\mathcal{I}} \cdot \boldsymbol{x} = \bigoplus_{i \in \mathcal{I}} (\boldsymbol{x} \lll i),$$

where $\boldsymbol{x}$ is the $(n \cdot b)$-bit input vector.

This diffusion primitive has been used in symmetric-key ciphers SMS4 [DL08], DBlock [WZY15] and RoadRunneR [BS15]. For example, SMS4 adopts an MDS $M_{4,8}^{\mathcal{I}}$ where $\mathcal{I}= \{0, 2, 10, 18, 24\}$. Based on Proposition 2, the computation for judging whether $M_{n,b}^{\mathcal{I}}$ is perfect would be complicated[1] when $n$ is large. So the focus of this paper is placed only on $4 \times 4$ linear layers, which are widely used in the modern cryptography.

It is not difficult to see that rotational-XOR matrix is a specific type of circulant matrices, and $M_{4,b}^{\mathcal{I}}$ can be expressed as

$$Circ(A, B, C, D) = \begin{bmatrix} A & B & C & D \\ D & A & B & C \\ C & D & A & B \\ B & C & D & A \end{bmatrix},$$

where $A$, $B$, $C$ and $D$ are all $b \times b$ matrices over $\mathbb{F}_2$. Just as mentioned in [DKR97, SKOP15], using circulant matrix in a diffusion layer has significant advantages, e.g. the prominent flexibility to be implemented in both round-based and serialized implementations. Nevertheless, it must be noticed that $M_{4,b}^{\mathcal{I}}$ is a bit-wise cyclic matrix, while it is not the case for the general circulant matrix (e.g. recent constructions in [LW16] and [LS16]).

**Proposition 3.** *If $M_{4,8}^{\mathcal{I}}$ is an MDS matrix (i.e. $\mathcal{B}_d(M_{4,8}^{\mathcal{I}}) = 5$) for some set $\mathcal{I}$, then $|\mathcal{I}| \geq 5$.*

Although the result above has been proved only for $b = 8$ in [ZWFS09], it can be extended for arbitrary size $b$ in a trivial way, and we ignore the proof here. Due to the MDS diffusion layers used in SMS4 and DBlock, the lower bound provided by Proposition 3 is tight. More importantly, as shown later in this paper, we are always able to construct perfect $M_{4,b}^{\mathcal{I}}$ as long as $b \geq 4$, implying that this lower bound is tight also for any $b \geq 4$. As a consequence, in view of the lightweight hardware/software implementation, we mainly study the construction of $M_{4,b}^{\mathcal{I}}$ with $|\mathcal{I}| = 5$ in the remaining sections.

## 3 On Properties of Rotational-XOR Diffusion Layers

Before giving our novel observations, we need to introduce some notations. For a $b \times b$ binary matrix $A = (a_{i,j})$ where $1 \leq i, j \leq b$, we say $A$ has diagonal $\sigma$, if $a_{i,j} = 1$ for all $i$ and $j$ such that $j - i = \sigma$. Furthermore, if $A$ has diagonals $\sigma_1, ..., \sigma_t$, and has no 1 at other positions, we use the expression

$$A = \sum_{i=1}^{t} diag(\sigma_i)$$

[1] As can be deduced from [GWG15], the time complexity is about $nb^3 \cdot \sum_{i=1}^{\mathcal{B}_d} (i^2 \cdot C_{2n}^i)$ to deal with such a matrix with branch number $\mathcal{B}_d$.

for simplicity. As an illustration, binary matrix shown in Figure 1-($a$) can be denoted by $diag(7) + diag(0) + diag(-5)$.

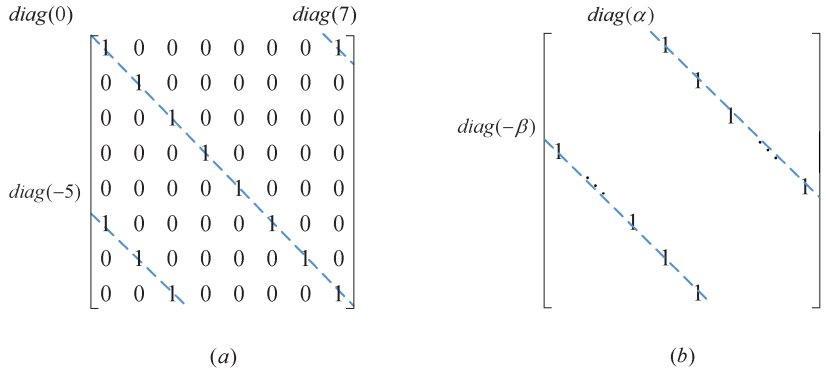


**Figure 1:** Binary matrices with element 1 only at diagonals

Let $A = diag(\alpha) + diag(-\beta)$ be a $b \times b$ non-singular binary matrix, where $\alpha, \beta > 0$. Note that there are $b-\alpha$ and $b-\beta$ 1's in the diagonal $\alpha$ and $\beta$ respectively. We claim that $\alpha + \beta \leq b$. Otherwise, the number of element 1 is less than $b$, and $A$ is obviously singular. Now we deduce a necessary and sufficient condition for such matrix to be invertible.

**Theorem 1.** *A $b \times b$ binary matrix $A = diag(\alpha) + diag(-\beta)$, $\alpha, \beta > 0$, is non-singular if and only if $(\alpha + \beta)|b$.*

*Proof.* As depicted in Figure 1-($b$), all row vectors of $A$, $\boldsymbol{a}_1, ..., \boldsymbol{a}_b$, can be divided into three groups:

(1) $\boldsymbol{a}_1 = \boldsymbol{e}_{\alpha+1},\ \ldots\ ,\ \boldsymbol{a}_\beta = \boldsymbol{e}_{\alpha+\beta}$.

(2) $\boldsymbol{a}_{\beta+1} = \boldsymbol{e}_{\alpha+\beta+1} + \boldsymbol{e}_1,\ \ldots\ ,\ \boldsymbol{a}_{b-\alpha} = \boldsymbol{e}_b + \boldsymbol{e}_{b-\alpha-\beta}$.

(3) $\boldsymbol{a}_{b-\alpha+1} = \boldsymbol{a}_{b-\alpha-\beta+1},\ \ldots\ ,\ \boldsymbol{a}_b = \boldsymbol{e}_{b-\beta}$.

$A$ is invertible if and only if each row vector $\boldsymbol{e}_i$, $1 \leq i \leq b$, can be represented as a linear combination of these $\boldsymbol{a}_j$'s. Let

$$\Omega = \Omega_1 \cup \Omega_2 = \{\alpha + 1, \cdots, \alpha + \beta\} \cup \{b - \alpha - \beta + 1, \cdots, b - \beta\}.$$

First, it holds for $\boldsymbol{e}_1$ that

$$\begin{aligned} \boldsymbol{e}_1 &= \boldsymbol{a}_{\beta+1} + \boldsymbol{e}_{\alpha+\beta+1} \\ &= \boldsymbol{a}_{\beta+1} + \boldsymbol{a}_{2\beta+\alpha+1} + \boldsymbol{e}_{2(\alpha+\beta)+1} \\ &= \cdots \\ &= \boldsymbol{a}_{\beta+1} + \cdots + \boldsymbol{a}_{t\beta+(t-1)\alpha+1} + \boldsymbol{e}_{t(\alpha+\beta)+1}, \end{aligned}$$

and $\boldsymbol{e}_1$ can be expressed as a linear combination of the $\boldsymbol{a}_j$'s if and only if there exists some index $t(\alpha + \beta) + 1$ such that $\boldsymbol{e}_{t(\alpha+\beta)+1} = \boldsymbol{a}_{j_1}$, i.e. $t(\alpha + \beta) + 1 \in \Omega$. Thereupon

$$\boldsymbol{e}_1 = \boldsymbol{a}_{\beta+1} + \boldsymbol{a}_{2\beta+\alpha+1} + \cdots + \boldsymbol{a}_{t\beta+(t-1)\alpha+1} + \boldsymbol{a}_{j_1}.$$

It should also be noticed that for each $\boldsymbol{e}_{i_1}$ with $i_1 = 1 \bmod (\alpha + \beta)$, $\boldsymbol{e}_{i_1}$ is expressible in the similar way.

Likewise, for other standard unit vectors, $\boldsymbol{e}_i$ can be represented as a linear combination of $\boldsymbol{a}_j$'s, if and only if there exists some $j_i \in \Omega$ such that $j_i = i \bmod (\alpha + \beta)$. Since $\Omega_1$

and $\Omega_2$ are disjoint (otherwise there would be two identical rows in $A$), then $|\Omega| = \alpha + \beta$, which implies $\Omega$ forms a complete residue system modulo $\alpha + \beta$. Moreover, as both $\Omega_1$ and $\Omega_2$ consist of consecutive integers, it must hold that

$$(b - \alpha - \beta + 1) \bmod (\alpha + \beta) = (\alpha + \beta) \bmod (\alpha + \beta) + 1,$$

which is equivalent to $b \bmod (\alpha + \beta) = 0$. Thereby, $(\alpha + \beta)|b$ is a necessary and sufficient condition for $A$ to be invertible. □

Note that if $A = diag(0) + diag(t)$ where $t \neq 0$, $A$ is always invertible. Thus we can obtain the sufficient and necessary conditions for invertibility of matrices containing only two diagonals.

**Corollary 1.** *Let $A = diag(\alpha) + diag(\beta)$ be a $b \times b$ matrix. $A$ is invertible if and only if one of the following conditions is satisfied.*

*(1) $\alpha \neq \beta$ and one of them is 0.*

*(2) $\alpha\beta < 0$ and $|\alpha - \beta|$ is a divisor of $b$.*

**Theorem 2.** *A $b \times b$ matrix $A = diag(0) + diag(t)$, $t \neq 0$, is involutory if and only if $|t| \geq \lceil b/2 \rceil$.*

*Proof.* Since the transpose of an involutory matrix is still involutory, we only consider the case $t > 0$. First, all row vectors of $A$ can be denoted by

$$\boldsymbol{a}_1 = \boldsymbol{e}_1 + \boldsymbol{e}_{t+1},\ \ldots\ ,\ \boldsymbol{a}_{b-t} = \boldsymbol{e}_{b-t} + \boldsymbol{e}_b,\ \boldsymbol{a}_{b-t+1} = \boldsymbol{e}_{b-t+1},\ \ldots\ ,\ \boldsymbol{a}_b = \boldsymbol{e}_b,$$

and all column vectors can be denoted by

$$\boldsymbol{a}'_1 = \boldsymbol{e}_1,\ \ldots\ ,\ \boldsymbol{a}'_t = \boldsymbol{e}_t,\ \boldsymbol{a}'_{t+1} = \boldsymbol{e}_{t+1} + \boldsymbol{e}_1,\ \ldots\ ,\ \boldsymbol{a}'_b = \boldsymbol{e}_b + \boldsymbol{e}_{b-t}.$$

Let $H = A^2$, and then $H_{i,j}$ is the inner product of the $i$-th row and $j$-th column of $A$. It is easy to see that

$$H = I \Leftrightarrow < \boldsymbol{a}_i, \boldsymbol{a}'_j >= \delta_{ij} \Leftrightarrow t + 1 > b - t,$$

where $\delta_{ij}$ is the Kronecker delta. This means $A^2 = I$ is equivalent to

$$t \geq \begin{cases} (b+1)/2 & b \text{ is odd} \\ b/2 & b \text{ is even,} \end{cases}$$

and we complete the proof. □

Next, by exploiting the properties of rotational-XOR diffusion layers $M^{\mathcal{I}}_{4,b}$ with $|\mathcal{I}| = 5$, we find ways to group them in equivalent classes.

**Proposition 4.** *Let $M^{\mathcal{I}}_{4,b}$ be a rotational-XOR matrix with $\mathcal{I} = \{i_1, ..., i_5\}$, $0 \leq i_1 < \cdots < i_5 \leq 4b - 1$. $M^{\mathcal{I}}_{4,b}$ has the same branch number with $M^{\mathcal{I}'}_{4,b}$, where $\mathcal{I}' = \{(i_1 + b) \bmod 4b, ..., (i_5 + b) \bmod 4b\}$.*

As a matter of fact, Proposition 4 indicates a right rotation on the 4 blocks of $Circ(A, B, C, D)$. In addition, left rotation by $i$ bits is equivalent to right rotation by $4b - i$ bits for any $4b$-bit vector, and intuitively there should not be any difference between left rotation and right rotation in terms of the branch number. Therefore we obtain the result below.

**Proposition 5.** *Let $M^{\mathcal{I}}_{4,b}$ be a rotational-XOR matrix with $\mathcal{I} = \{i_1, ..., i_5\}$, $0 \leq i_1 < \cdots < i_5 \leq 4b - 1$. $M^{\mathcal{I}}_{4,b}$ and $M^{\mathcal{I}'}_{4,b}$ are of the same branch number, where $\mathcal{I}' = \{(4b - i_1) \bmod 4b, ..., (4b - i_5) \bmod 4b\}$.*

*Proof.* Note that $M_{4,b}^{\mathcal{I}'}$ is closely related to the transpose of $M_{4,b}^{\mathcal{I}}$. More precisely,

$$M_{4,b}^{\mathcal{I}'} = Circ(A^T, D^T, C^T, B^T).$$

Let $P = (\boldsymbol{e}_b, ..., \boldsymbol{e}_1)$. For persymmetric matrix $A$, we have $A^T = PAP$. According to Proposition 1 and Proposition 4, $M_{4,b}^{\mathcal{I}'}$ and $M_{4,b}^{\mathcal{I}}$ are of the same branch number since $P$ is invertible. □

In the sequel, we always assume that $i_1 = 0$. For cases where $i_1 > 0$,[2] search results and some other evidences suggest it is very likely that $M_{4,b}^{\mathcal{I}}$ is not MDS. Unfortunately, at the time being, we could not find a rigorous and complete proof for the assertion. Nevertheless, we can show that when $i_1 = 0$, there always exists an $M_{4,b}^{\mathcal{I}'}$ which is equivalent to $M_{4,b}^{\mathcal{I}}$ such that $i'_1 = 0$ and $i'_2 < b$. Indeed, if $i_2 < b$ then $\mathcal{I}' = \mathcal{I}$ and we are done. Otherwise, it holds that $i_2 = b$ in order for $B$ to be invertible. If $i_3 < 2b$, we set $\mathcal{I}' = \{(i_1 - b) \bmod 4b, ..., (i_5 - b) \bmod 4b\} = \{0, i_3 - b, i_4 - b, i_5 - b, i_1 + 3b\}$, and we are done. Continuing this procedure, we can always find a block with exactly two non-negative diagonals, one of which is diagonal 0. Thus, we have proved that:

**Theorem 3.** *For any MDS $M_{4,b}^{\mathcal{I}} = Circ(A, B, C, D)$ which contains at least one diagonal 0 among the five non-negative diagonals, there always exists an $M_{4,b}^{\mathcal{I}'} = Circ(A', B', C', D')$ where $A' = diag(\sigma) + diag(0)$ and $\sigma > 0$, such that $\mathcal{B}_d(M_{4,b}^{\mathcal{I}'}) = \mathcal{B}_d(M_{4,b}^{\mathcal{I}})$.*

Furthermore, for any rotational-XOR MDS diffusion layer $M_{4,b}^{\mathcal{I}}$ with $|\mathcal{I}| = 5$, we claim that there are at most two indices in $\mathcal{I} = \{i_1, ..., i_5\}$ divisible by $b$. Suppose not, two cases should be discussed:

(1) If there are four indices in $\mathcal{I}$ divisible by $b$, then without loss of generality, we consider the case visualized in Figure 2. Here $A = B$ and $B + C$ is singular. Hence there obviously exists a non-zero vector $\boldsymbol{x} = (\boldsymbol{e}_1, \boldsymbol{e}_1, \mathbf{0}, \mathbf{0})$ such that $wt(\mathbf{x}) + wt(M_{4,b}^{\mathcal{I}} \cdot \mathbf{x}) \leq 4$, which contradicts the MDS condition.

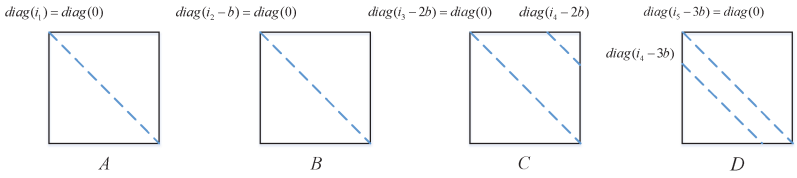


**Figure 2:** $M_{4,b}^{\mathcal{I}}$ with $|\mathcal{I}| = 5$ where there exist four indices in $\mathcal{I}$ divisible by $b$

(2) If there are three indices in $I$ divisible by $b$, without loss of generality, assume that $b|i_1$, $b|i_2$, $b|i_3$. Then in order for $D$ being invertible, there are two possible situations.

(i) $i_4 < 3b$ and $i_5 = i_4 + b$. We notice that either $A$ or $C$ is involutory,[3] and that $D = A + C$. Without loss of generality, suppose $A$ is involutory. As depicted in Figure 3-(i), $A^2 + A + C = I + A + C$ is singular (each row of the matrix has two 1's), so there exists a nonzero vector $\boldsymbol{x}$ such that $(A^2 + A + C)\boldsymbol{x} = \mathbf{0}$ (for example, $\boldsymbol{x}$ could be the all-one vector $(1, 1, ..., 1)$). Take $\boldsymbol{y} = A\boldsymbol{x}$, then $D\boldsymbol{x} + A\boldsymbol{y} = (A + C + A^2)\boldsymbol{x} = \mathbf{0}$ and $A\boldsymbol{x} + B\boldsymbol{y} = A\boldsymbol{x} + \boldsymbol{y} = \mathbf{0}$, which implies $wt(\boldsymbol{v}) + wt(M\boldsymbol{v}) \leq 4$ for the input $\boldsymbol{v} = (\boldsymbol{x}, \boldsymbol{y}, \mathbf{0}, \mathbf{0})$. This contradicts the MDS condition.

[2]From the perspective of equivalence class, now we are referring to cases where all indices in $\mathcal{I}$ are not divisible by $b$.

[3]Let $t_a$ and $t_c$ be the non-zero diagonals in $A$ and $C$ respectively. Then $t_a = i_4 - 3b$ and $t_c = i_4 - 2b$ based on Figure 3-(i). Since $|t_a| + |t_c| = b$, one of $|t_a|$ and $|t_c|$ must be no less than $b/2$. According to Theorem 2, either $A$ or $C$ is involutory.

(ii) $5/2b < i_4 < 3b$ and $i_5 = i_4 + s$, where $s > 3b - i_4$ is a proper divisor of $b$. As shown in Figure 3-(ii), $A + B$ and $B + C$ are singular matrices with common nonempty null space. Similar to the explication of case (i), the branch number of resulting matrix is no more than 4.

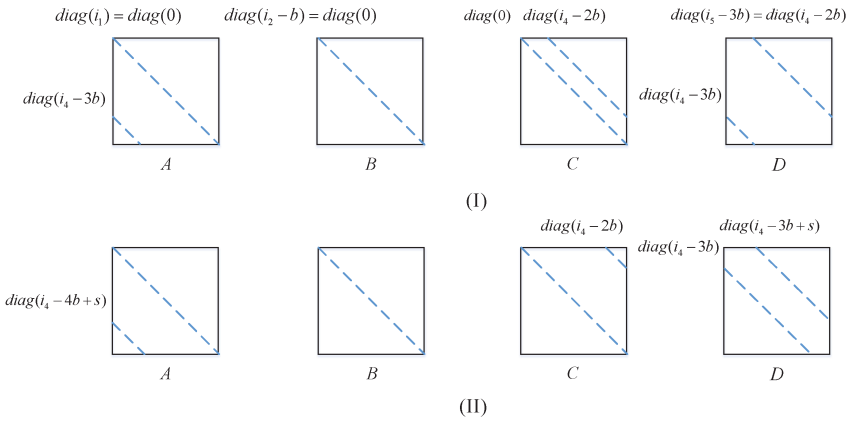


**Figure 3:** $M^{\mathcal{I}}_{4,b}$ with $|\mathcal{I}| = 5$ where there are three indices in $\mathcal{I}$ divisible by $b$

In summary, for an arbitrary MDS $M^{\mathcal{I}}_{4,b}$ with $|\mathcal{I}| = 5$, there are at most two indices in $\mathcal{I}$ divisible by $b$. As can be seen from the following elaboration, this is a crucial criterion which plays a significant role in determining the possible forms for perfect rotational-XOR diffusion layers.

# 4 On Forms of Rotational-XOR MDS Diffusion Layers

In this section, we illustrate possible forms of rotational-XOR MDS diffusion layers. Based on the analysis of Section 3, we can always restrict constructions to $M^{\mathcal{I}}_{4,b} = Circ(A, B, C, D)$ with $i_1 = 0$ and $0 < i_2 < b$. One such instance is naturally regarded as a representative, from which we can obtain some other candidates.

For the five shifts (or indices) in a set $\mathcal{I}$, consider all distances between two consecutive shifts where neither of the two shifts are divisible by $b$. In order for each block to be invertible, these distances should be a divisor of $b$, and at most one of them is strictly smaller than $b$. Due to such limits, there are only 7 possible forms of rotational-XOR MDS diffusion layers. We characterize the shifts for each possible form as follows:

(1) $\{0, l, l + b, l + s + b, l + s + 2b\}$,

(2) $\{0, l, l + s, l + s + b, l + s + 2b\}$,

(3) $\{0, l, l + b, l + s + b, 3b\}$,

(4) $\{0, l, l + s, l + s + b, 3b\}$,

(5) $\{0, l, l + b, l + 2b, l + s + 2b\}$,

(6) $\{0, l, l + b, l + 2b, l + 3b\}$,

(7) $\{0, l, l + b, l + 2b, 3b\}$,

where $0 < l < b$ and $s$ is a proper divisor of $b$. For ease of understanding, we describe the four blocks in the first row for each case in Appendix A.

There are some implicit points we should be aware of. First, $l$ in the first five cases must satisfy $l > b/2$.[4] Second, form (3) and (4) are equivalent according to Proposition 5, i.e. each instance in form (3) has an equivalent counterpart in form (4) and vice versa. Additionally, the last three blocks in form (6) are identical, which means it can not be MDS [LS16]. All these insights leave us only 5 cases (i.e. form (1), (2), (3), (5) and (7)) to detect.

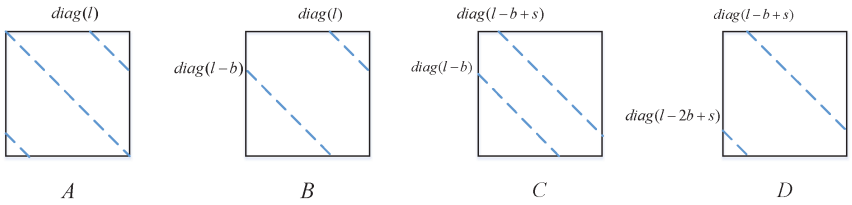


**Figure 4:** Rotational-XOR diffusion layer $M^{\mathcal{I}}_{4,b}$ with $\mathcal{I} = \{0, l, l+b, l+s+b, l+s+2b\}$

**Lemma 1.** *For $\mathcal{I} = \{0, l, l+b, l+s+b, l+s+2b\}$, where $l > b/2$, $M^{\mathcal{I}}_{4,b}$ is not MDS.*

*Proof.* Consider the sub-matrix $T = \begin{bmatrix} B & D \\ D & B \end{bmatrix}$, we prove that $B + D$ is singular, so $T$ is singular. As shown in Figure 4,

$$B + D = diag(l - b) + diag(l) + diag(l + s - 2b) + diag(l + s - b).$$

Then $B + D$ has exactly two 1's in each row, which means the sum of all columns of $B + D$ is $\mathbf{0}$ since we are working over $\mathbb{F}_2$. As a result, $B + D$ is singular, implying that $M^{\mathcal{I}}_{4,b}$ is not MDS. □

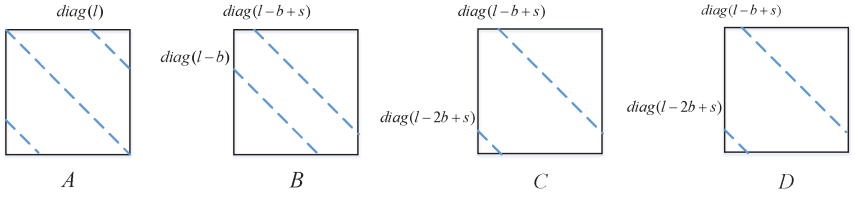


**Figure 5:** Rotational-XOR diffusion layer $M^{\mathcal{I}}_{4,b}$ with $\mathcal{I} = \{0, l, l+s, l+s+b, l+s+2b\}$

**Lemma 2.** *For $\mathcal{I} = \{0, l, l+s, l+s+b, l+s+2b\}$, where $l > b/2$, $M^{\mathcal{I}}_{4,b}$ is not MDS.*

*Proof.* It is not difficult to see that $C$ and $D$ are identical, and that $B + C$ is singular since it is lower-triangular (See Figure 5). Then there must exist a nonzero $\boldsymbol{x}$ such that $(B + C)\boldsymbol{x} = \mathbf{0}$. As $(C + D)\boldsymbol{x} = \mathbf{0}$ also holds, the vector $\boldsymbol{v} = (\mathbf{0}, \mathbf{0}, \boldsymbol{x}, \boldsymbol{x})$ results in $wt(\boldsymbol{v}) + wt(M^{\mathcal{I}}_{4,b}\boldsymbol{v}) \leq 4$, which is a contradiction. □

**Lemma 3.** *For $\mathcal{I} = \{0, l, l+b, l+s+b, 3b\}$, where $l > b/2$, $M^{\mathcal{I}}_{4,b}$ is not MDS.*

*Proof.* Note that $s \leq b/2 < l$. Consider the sub-matrix $T = \begin{pmatrix} B & C \\ D & A \end{pmatrix} \triangleq \begin{pmatrix} T_1 & T2 \end{pmatrix}$ and column vector $\boldsymbol{v} = (\boldsymbol{e}_b + \boldsymbol{e}_{l+s-b} + \boldsymbol{e}_s, \boldsymbol{e}_{l+s-b} + \boldsymbol{e}_s)$. After labeling the diagonals (See

[4] For each block to be invertible, it holds that $l + s \geq b$. According to the previous discussion, the intermediate blocks (i.e. $B$ and $C$) do not have diagonal 0, which implies $l + s$ is strictly larger than $b$. Thereby $l > b/2$ since $s$ is a proper divisor of $b$ (which is at most $b/2$).

Figure 6), we make simple computations to obtain that the $(l+s-b)$-th column of $T_1$ is $\boldsymbol{e}_s + \boldsymbol{e}_{l+s} + \boldsymbol{e}_{2b}$, the $s$-th column of $T_1$ is $\boldsymbol{e}_{b+s-l} + \boldsymbol{e}_{s+b}$, and the $b$-th column of $T_1$ is $\boldsymbol{e}_{b-l} + \boldsymbol{e}_{2b}$. Similarly, the $(l+s-b)$-th and $s$-th columns of $T_2$ are $\boldsymbol{e}_s + \boldsymbol{e}_{l+s}$ and $\boldsymbol{e}_{s-l+b} + \boldsymbol{e}_{b-l} + \boldsymbol{e}_{s+b}$ respectively. Since the sum of all these columns is $\mathbf{0}$, i.e. $T\boldsymbol{v} = \mathbf{0}$, $T$ is singular and $M^{\mathcal{I}}_{4,b}$ is not MDS. □

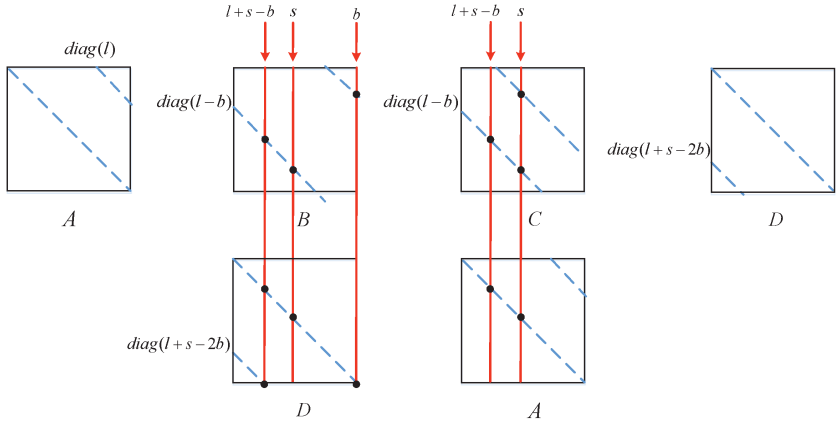


**Figure 6:** Singular sub-matrix in $M^{\mathcal{I}}_{4,b}$ with $\mathcal{I} = \{0, l, l+b, l+s+b, 3b\}$

**Lemma 4.** *For $\mathcal{I} = \{0, l, l+b, l+2b, l+s+2b\}$, where $l > b/2$, $M^{\mathcal{I}}_{4,b}$ is not MDS.*

We can prove Lemma 4 in a similar way to Lemma 2. After eliminating all the other case, we find the only possible candidate rotational-XOR MDS diffusion layer $M^{\mathcal{I}}_{4,b}$, with $|\mathcal{I}| = 5$ and $i_1 = 0$.

**Theorem 4.** *Any rotational-XOR MDS diffusion layer $M^{\mathcal{I}}_{4,b}$, with $|\mathcal{I}| = 5$ and $i_1 = 0$, must satisfy that*

$$\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$$

*for some $0 < l < b$ from a equivalent point of view.*

We will later give the sufficient and necessary conditions for such $M^{\mathcal{I}}_{4,b}$ to be MDS. According to our result, we can recognize that for any $b \geq 4$, there always exists rotational-XOR MDS diffusion layer $M^{\mathcal{I}}_{4,b}$ with $|\mathcal{I}| = 5$, which prove the tightness for the bound of cardinality of $\mathcal{I}$.

**Corollary 2.** *If $M^{\mathcal{I}}_{n,b}$, $n > 4$, is a rotational-XOR MDS diffusion layer, $|\mathcal{I}| \geq n + 2$.*[5]

## 5 Direct Construction of Rotational-XOR MDS Diffusion Layers

In this section, we deduce a direct construction of MDS $M^{\mathcal{I}}_{4,b}$ with $|\mathcal{I}| = 5$. Along the same line, all perfect linear layers are of the form $Circ(A, B, B, A+B)$, where $A = diag(0) + diag(l)$ and $B = diag(l) + diag(l-b)$.

[5]Since the proof process is a little repetitive, we describe it in Appendix B.

### 5.1 Direct construction of MDS $M_{4,b}^{\mathcal{I}}$ with $\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$

By exhaustive search of all square sub-matrices of $M$, we obtain the result below.

**Lemma 5.** *Let $M = Circ(A, B, B, A+B)$ be a circulant matrix with $A, B, A+B \in GL(b, \mathbb{F}_2)$. Then $M$ is an MDS matrix if and only if the following three statements hold.*

*(1)* $|A + B + BA^{-1}B| \neq 0$.

*(2)* $|A + B + BA^{-1}BA^{-1}B| \neq 0$.

*(3)* $|A + BA^{-1}B + BA^{-1}BA^{-1}B| \neq 0$.

*Proof.* According to Proposition 2, $M$ is an MDS matrix if and only if all square sub-matrices of order $t$, $1 \leq t \leq 4$, are non-singular. With the help of elementary linear algebra, we obtain $|M| = |B|^4$, which implies conditions for the case of $t = 1$ and $t = 4$ are trivially satisfied. To ensure all square sub-matrices of order 2 are invertible, we further require $|A + B + BA^{-1}B| \neq 0$. Similarly, for the case of $t = 3$, not only $|A|$, $|B|$ and $|A + B|$, but also the three determinants above need to be non-zero. □

*Remark* 1. Note that the forms of these three determinants are not unique due to the varying procedure of computation. Nevertheless, all possible determinants we compute are equivalent to these three under the condition that $A, B, A + B$ are all invertible.

Next, we elaborate on a necessary and sufficient condition for each nontrivial determinant being non-zero.

**Theorem 5.** *Assume $A = diag(0) + diag(l)$ and $B = diag(l) + diag(l - b)$ are two $b \times b$ binary matrices where $0 < l < b$. Then $|A + B + BA^{-1}BA^{-1}B|$ is non-zero if and only if $l \neq 3b \bmod 7$.*

*Proof.* According to the definitions, it is easy to see $|A| \neq 0$, $|B| \neq 0$, and thus it holds that

$$|A + B + BA^{-1}BA^{-1}B| \neq 0 \Leftrightarrow |I + A^{-1}B + A^{-1}BA^{-1}BA^{-1}B| \neq 0.$$

Let $W = A^{-1}B$, then

$$I + A^{-1}B + A^{-1}BA^{-1}BA^{-1}B = I + W + W^3.$$

On the one hand, for any eigenvalue of $W$, denoted by $\lambda$, it satisfies $|\lambda I - U| = 0$, which is equivalent to $\lambda^b + (\lambda + 1)^{b-l} = 0$ since

$$\lambda A - B = \begin{bmatrix} \lambda & & \lambda+1 & & \\ & \lambda & & \ddots & \\ & & & & \lambda+1 \\ 1 & & \ddots & & \\ & \ddots & & & \\ & & 1 & & \lambda \end{bmatrix}.$$

On the other hand, based on linear algebra theory, $I + W + W^3$ is non-singular if and only if $1 + \lambda + \lambda^3 \neq 0$. Now we consider the opposite direction, i.e. we compute the conditions for $1 + \lambda + \lambda^3 = 0$. Notice that $1 + \lambda + \lambda^3$ is a primitive polynomial of order 7 over $\mathbb{F}_2$, and $\lambda + 1 = \lambda^3$. Then we obtain

$$\lambda^b + (\lambda + 1)^{b-l} = 0 \Leftrightarrow \lambda^b + \lambda^{3(b-l)} = 0 \Leftrightarrow b = 3(b - l) \bmod 7.$$

Therefore, $I + W + W^3$ is non-singular if and only if $l \neq 3b \bmod 7$, and we complete the proof. □

Likewise, we claim that $|A + B + BA^{-1}B| \neq 0$ if and only if $l \neq 2b \bmod 3$, and $|A + BA^{-1}B + BA^{-1}BA^{-1}B| \neq 0$ if and only if $l \neq 5b \bmod 7$. The relevant explications are similar to the proof above, except that primitive polynomials are changed (from $1 + \lambda + \lambda^3$) to $1 + \lambda + \lambda^2$ and to $1 + \lambda^2 + \lambda^3$ respectively.

**Theorem 6.** *Let $A = diag(0) + diag(l)$ and $B = diag(l) + diag(l - b)$ be two $b \times b$ binary matrices, where $0 < l < b$. A rotational-XOR diffusion layer $M^{\mathcal{I}}_{4,b}$ denoted by $Circ(A, B, B, A + B)$ is MDS, if and only if all conditions below are fulfilled.*

*(1)* $l \neq 2b \bmod 3$.

*(2)* $l \neq 3b \bmod 7$.

*(3)* $l \neq 5b \bmod 7$.

This statement is an immediate combination of Lemma 5 and Theorem 5, so we omit the proof here. According to Theorem 6, we deduce a direct construction of rotational-XOR MDS diffusion layers, without any auxiliary search. Indeed, once $b$ is given, the set of candidates for $l$ is determined:

$$\Lambda = \{l | 0 < l < b, l \neq 2b \bmod 3, l \neq 3b \bmod 7, l \neq 5b \bmod 7\}.$$

In other words, an arbitrary $l \in \Lambda$ corresponds to a perfect rotational diffusion layer $M^{\mathcal{I}}_{4,b}$, where $\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$. Alternatively, $M^{\mathcal{I}}_{4,b}$ can be represented as $Circ(A, B, B, A+B)$, where $A = diag(0) + diag(l)$, $B = diag(l) + diag(l - b)$.

## 5.2 The inverse of proposed diffusion layers

At the end of this section, we present the inverse of rotational-XOR diffusion layers constructed in Section 5.1.

**Theorem 7.** *Let $M^{\mathcal{I}}_{4,b} \cdot \boldsymbol{x} = \boldsymbol{x} \oplus (\boldsymbol{x} \lll l) \oplus (\boldsymbol{x} \lll (l + b)) \oplus (\boldsymbol{x} \lll (l + 2b)) \oplus (\boldsymbol{x} \lll 3b)$ and $\boldsymbol{x} \in (\mathbb{F}_2^b)^4$, $0 < l < b$. Then*

$$\begin{aligned}(M^{\mathcal{I}}_{4,b})^{-1} \cdot \boldsymbol{x} \;=\; & (\boldsymbol{x} \lll (4b - 4l)) \oplus (\boldsymbol{x} \lll (b - 4l)) \oplus (\boldsymbol{x} \lll (4b - l)) \oplus \\ & (\boldsymbol{x} \lll (3b - 4l)) \oplus (\boldsymbol{x} \lll (b - 3l)) \oplus (\boldsymbol{x} \lll (b - 2l)) \oplus \\ & (\boldsymbol{x} \lll (2b - 2l)) \oplus (\boldsymbol{x} \lll (2b - l)) \oplus (\boldsymbol{x} \lll (3b - l)) \oplus \\ & (\boldsymbol{x} \lll (3b - 3l)) \oplus (\boldsymbol{x} \lll (2b - 4l))\end{aligned}$$

*where $\boldsymbol{x} \lll i$ is equivalent to $\boldsymbol{x} \lll (i \bmod 4b)$.*

*Proof.* Starting from the expression of $M^{\mathcal{I}}_{4,b} \cdot \boldsymbol{x}$, we have

$$\begin{aligned}(M^{\mathcal{I}}_{4,b})^2 \cdot \boldsymbol{x} &= \boldsymbol{x} \oplus (\boldsymbol{x} \lll 2l) \oplus (\boldsymbol{x} \lll (2l + 2b)) \oplus (\boldsymbol{x} \lll (2l + 4b)) \oplus (\boldsymbol{x} \lll 6b) \\ &= \boldsymbol{x} \oplus (\boldsymbol{x} \lll 2b) \oplus (\boldsymbol{x} \lll (2l + 2b)).\end{aligned}$$

Furthermore, $(M^{\mathcal{I}}_{4,b})^4 \cdot \boldsymbol{x} = \boldsymbol{x} \oplus (\boldsymbol{x} \lll (4l + 4b)) \oplus (\boldsymbol{x} \lll 4b) = \boldsymbol{x} \lll 4l$, implying that

$$(M^{\mathcal{I}}_{4,b})^4 \cdot (\boldsymbol{x} \lll (4b - 4l)) = \boldsymbol{x}.$$

Consequently, it holds that

$$(M^{\mathcal{I}}_{4,b})^{-1} \cdot \boldsymbol{x} = (M^{\mathcal{I}}_{4,b})^3 \cdot (\boldsymbol{x} \lll (4b - 4l)) = ((M^{\mathcal{I}}_{4,b})^2 \cdot M^{\mathcal{I}}_{4,b}) \cdot (\boldsymbol{x} \lll (4b - 4l)),$$

which completes the proof. □

*Remark* 2. As can be seen from $(M_{4,b}^{\mathcal{I}})^2$, any rotational-XOR MDS diffusion layer we construct cannot be involutory.

**Corollary 3.** *Assume* $M_{4,b}^{\mathcal{I}'} = (M_{4,b}^{\mathcal{I}})^{-1}$ *and* $\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$. *Any two terms in* $\mathcal{I}'$ *are not congruent modulo* $4b$.

*Proof.* Let $\mathcal{I}'_1 = \{2b-l, 3b-l, 4b-l\}$, $\mathcal{I}'_2 = \{b-2l, 2b-2l\}$, $\mathcal{I}'_3 = \{b-3l, 3b-3l\}$ and $\mathcal{I}'_4 = \{b-4l, 2b-4l, 3b-4l, 4b-4l\}$. According to Theorem 7,

$$\mathcal{I}' = \mathcal{I}'_1 \cup \mathcal{I}'_2 \cup \mathcal{I}'_3 \cup \mathcal{I}'_4.$$

Elements from the same $\mathcal{I}'_j$, $1 \le j \le 4$, are not congruent modulo $4b$.

If two elements are congruent modulo $4b$, they must come from different set $\mathcal{I}'_i$, $\mathcal{I}'_j$, $i \neq j$. Suppose $kb - il = rb - jl \bmod 4b$, and $k, r$ are possible coefficients of $b$ in $\mathcal{I}'_i$, $\mathcal{I}'_j$. Then

$$(k-r)b = (i-j)l \bmod 4b.$$

Since $0 < l < b$, the only possibility is $l = b/2$, which implies $l = 2b \bmod 3$. This contradicts the MDS condition for $M_{4,b}^{\mathcal{I}}$. □

*Remark* 3. Any two terms in $\mathcal{I}'$ are not congruent modulo $4b$, and then for a rotational-XOR MDS matrix we construct, its inverse matrix contains exactly 11 rotations.

# 6 Discussion and Implementation

Before comparing the implementation cost, we make a thorough discussion for various parameters. Since $M_{4,b}^{\mathcal{I}}$ is uniquely determined by $\mathcal{I}$, and the set $\mathcal{I}$ of each MDS matrix satisfies $\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$, we extract $l$ to illustrate our instances. For example, $M_{4,4}^{\mathcal{I}}$ with $l = 3$ can be characterized as

$$M_{4,4}^{\mathcal{I}} \cdot \boldsymbol{x} = \boldsymbol{x} \oplus (\boldsymbol{x} \lll 3) \oplus (\boldsymbol{x} \lll 7) \oplus (\boldsymbol{x} \lll 11) \oplus (\boldsymbol{x} \lll 12),$$

where $\boldsymbol{x}$ is a 16-bit input vector. For the other expression, $M_{4,4}^{\mathcal{I}}$ corresponds to the rotational-XOR linear layer $Circ(A, B, B, A+B)$, which is constructed by the following $4 \times 4$ matrices:

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

## 6.1 Rotational-XOR diffusion layers for various parameters

First, we utilize Theorem 6 to directly generate rotational-XOR MDS diffusion layers with commonly used sizes in the modern cryptography, that is, $M_{4,b}^{\mathcal{I}}$ with $b = 2^k$, where $k = 2, 3, 4, 5$. The total number of $l$ which satisfies conditions of Theorem 6 and typical instance of $\mathcal{I}$ are summarized in Table 1.

We point out that all these proposals listed in Table 1 are immediate results of Theorem 6. In other words, as there is no further partition, the number of equivalence classes for each parameter is smaller than the second item (i.e. the total number of $l$). For example, when $b = 16$, direct constructions from Theorem 6 are $l = 1, 4, 7, 9, 12$ and 15. While according to Proposition 5, they are pairwise equivalent. Namely, $l = 1$ and $l = 15$, $l = 4$ and $l = 12$, $l = 7$ and $l = 9$ belong to three different equivalent classes.

Next, we emphasize that our construction is applicable for any $b \ge 4$, and thereby it becomes possible for direct generating MDS $M_{4,b}^{\mathcal{I}}$ even for sizes which are not often used.

**Table 1:** Direct construction of MDS $M_{4,b}^{\mathcal{I}}$ with $b = 4$, 8, 16, and 32

| $b$ | total number of $l$ | example of $\mathcal{I}$ |
|---|---|---|
| 4 | 2 | $\{0, 1, 5, 9, 12\}$ |
| 8 | 2 | $\{0, 2, 10, 18, 24\}$ |
| 16 | 6 | $\{0, 7, 23, 39, 48\}$ |
| 32 | 14 | $\{0, 9, 41, 73, 96\}$ |

For example, when considering MDS $M_{4,5}^{\mathcal{I}}$, $\mathcal{I} = \{0, 2, 7, 12, 15\}$ and $\mathcal{I} = \{0, 3, 8, 13, 15\}$ are both perfect solutions. For $M_{4,7}^{\mathcal{I}}$, $\mathcal{I} = \{0, l, l + b, l + 2b, 3b\}$, to be MDS, $l = 1, 3, 4$ and 6 are all feasible choices.

Last, to confirm the validity of our construction, we make exhaustive search for MDS $M_{4,b}^{\mathcal{I}}$ with $b \leq 16$. Remarkably, our proposals for each parameter exactly covered the whole perfect instances (in the sense of equivalence). For example, experimental results show that there are in total 8 MDS $M_{4,8}^{\mathcal{I}}$'s with $|\mathcal{I}| = 5$, and their $\mathcal{I}$'s are

$$\{0, 2, 10, 18, 24\}, \{0, 8, 10, 18, 26\}, \{2, 8, 16, 18, 26\}, \{2, 10, 16, 24, 26\},$$

$$\{0, 6, 14, 22, 24\}, \{0, 8, 14, 22, 30\}, \{6, 8, 16, 22, 30\}, \{6, 14, 16, 24, 30\}.$$

According to Proposition 4, the first 4 matrices and last 4 matrices are in two different equivalence classes. This means exhaustive search result is consistent with our construction, since $\mathcal{I} = \{0, 2, 10, 18, 24\}$ and $\mathcal{I} = \{0, 6, 14, 22, 24\}$ are immediate solutions of Theorem 6.

## 6.2 XOR count and comparison with previous constructions

**XOR count** Hardware efficiency can have very different meanings depending on the utilization scenario targeted by designers. A classical metric is to estimate silicon area needed by the primitive to perform cryptographic operations. As expounded in [KPPY14], low XOR count is strongly correlated to the minimization of hardware area. Since all rows for a circulant matrix (and also for a Hadamard matrix) are equivalent in terms of XOR count, we use the amount of XORs required to evaluate the first row to evaluate the lightweightness of a given matrix. A comparison of our constructions with previous ones is given in Table 2. It is not difficult to see that our results are very close to the best existing constructions.

**Implementation tradeoffs** Since our construction uses a bit-wise circulant structure, there are various trade-offs in its implementation. All constructions in Table 2 use circulant (or circulant-like) structure, so the XOR costs of their unrolled implementations are 4 times higher than the row-based implementation. As a consequence, our results are still very similar to the best existing ones. In addition, our construction uses a bit-wise circulant structure, therefore its implementation allows more fine-grained trade-offs. In an extreme case, we can implement only the first output bit (rather than the first row), and then compute all the other bits through rotations.

Indeed, whichever instance we choose in our construction, the XOR cost is always proportional to the bit-width of current implementation. Specifically, for any $nb \times nb$ binay matrix, the XOR cost of the trivial unrolled implementation is $4nb$. As for the row-based implementation (in which we only compute one entry, i.e. $b$-bit, each time), this value becomes $4b$. Clearly, the ratio of total XOR cost versus implementation bit-width is a constant 4. For larger matrices (e.g. $nb = 64, 128, \cdots$), this nice property becomes a significant advantage: despite the fact that there are fewer methods for generating huge MDS, Table 2 indicates that the XOR cost of our direct construction should stay close to the best possible results.

**Table 2:** Comparison of MDS matrices with commonly used sizes

| Matrix type | Elements | The first row | XOR count | Reference |
|---|---|---|---|---|
| Hadamard | $\mathbb{F}_{2^4}/0x13$ | $(0x01, 0x02, 0x08, 0x09)$ | 17 | [SKOP15] |
| Hadamard | $GL(4, \mathbb{F}_2)$ | $(I, A, B, C)$ | 16 | [LW16] |
| Circulant | $GL(4, \mathbb{F}_2)$ | $(I, I, A, B)$ | 15 | [LW16] |
| Circulant | $\mathbb{F}_{2^4}/0x13$ | $(0x01, 0x01, 0x09, 0x04)$ | 15 | [LS16] |
| Circulant | $\mathbb{F}_{2^4}/0x13$ | $(0x01, 0x01, 0x04, 0x09)$ | 15 | [KPPY14] |
| Circulant | $GL(4, \mathbb{F}_2)$ | $(A, B, B, A + B)$ | 16 | This paper |
| Circulant | $\mathbb{F}_{2^8}/0x11b$ | $(0x02, 0x03, 0x01, 0x01)$ | 38 | [DR02] |
| Hadamard | $\mathbb{F}_{2^8}/0x1c3$ | $(0x01, 0x02, 0x04, 0x91)$ | 37 | [SKOP15] |
| Circulant | $\mathbb{F}_{2^8}/0x11b$ | $(0x01, 0x01, 0x04, 0x8e)$ | 33 | [KPPY14] |
| Circulant | $\mathbb{F}_{2^8}/0x1c3$ | $(0x01, 0x01, 0x02, 0x91)$ | 32 | [LS16] |
| Circulant | $GL(8, \mathbb{F}_2)$ | $(I, I, A, B)$ | 27 | [LW16] |
| Circulant | $GL(8, \mathbb{F}_2)$ | $(A, B, B, A + B)$ | 32 | This paper |

**Software performance** Though the current lightweight constructions focus mainly on hardware implementation, it would be a bonus if cryptographic primitives can also be efficiently implemented in software platforms, considering an encryption algorithm might be used in various platforms. Apparently, our construction favors implementations with $nb$-bit processors. For any $32 \times 32$ binary matrix in Table 2, computing a 32-bit output requires 4 XORs and 4 rotations, with no extra memory cost. As many 32-bit processors have built-in rotation instructions, performing such transformation takes only 8 instructions. However, other examples in Table 2 take at least $3 \times 4$ XORs, no matter how multiplication operation is implemented. Therefore, the trivial implementation of our construction on 32-bit platforms outperforms most previous ones.

In addition to the trivial implementation, there are various optimizations improving software performance. For example, utilizing the look-up table or the bit-slice technique may lead to more efficient implementation. However, those optimizations only make sense when we have plenty of memory or we need to encrypt many blocks.[6] Besides, in practice, both the large table look-up and the pack/unpack operation may take a long time to proceed. Even though such optimizations do improve the overall performance, our construction has similar performance as previous ones. But for 8-bit platforms, our proposal becomes less effective: since $nb$-bit rotations cannot be efficiently implemented in a $w$-bit processor ($w < nb$), both our $16 \times 16$ and $32 \times 32$ instances do not work well with 8-bit processors. Nevertheless, to date, few constructions perform well on all types of platforms: our work here is no exception.

# 7 Conclusion

In this paper, we study the construction of rotational-XOR MDS diffusion layer over $(\mathbb{F}_2^b)^4$. By presenting a series of theory on such type of matrices, we propose a powerful method to directly generate perfect $M_{4,b}^{\mathcal{I}}$ for arbitrary $b \geq 4$. From the designer's point of view, our strategy provides a quite comprehensive solution to the construction of such $4 \times 4$ MDS matrices. Despite of a few limitations, our proposal contributes to the diversity of diffusion primitives. As far as we know, it is the first time that lightweight rotational-XOR MDS diffusion layers have been constructed without any auxiliary search.

[6] Unless the cryptographic scheme is designed in a bit-slice manner.

## Acknowledgments

The authors would like to thank all anonymous referees for their valuable comments that greatly improve the manuscript. This work is supported by the National Basic Research Program of China (No.2013CB338002), National Natural Science Foundation of China (No.61379139, No.61672509, No.61232009), and National Cryptography Development Fund (MMJJ20170101).

## References

[AF14] Daniel Augot and Matthieu Finiasz. Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes. In *Fast Software Encryption, FSE 2014*, pages 3–17, 2014.

[Ber13] T.P. Berger. Construction of Recursive MDS Diffusion Layers from Gabidulin Codes. In *International Conference on Cryptology in India, INDOCRYPT 2013*, pages 274–285, 2013.

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

[BS15] Adnan Baysal and Sühap Sahin. Roadrunner: A Small and Fast Bitslice Block Cipher for Low Cost 8-Bit Processors. In *Lightweight Cryptography for Security and Privacy, LightSec 2015*, pages 58–76, 2015.

[Dav80] Philip J. Davis. Circulant Matrices. *Mathematics of Computation*, 35(152), 1980.

[DKR97] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The Block Cipher Square. In *Fast Software Encryption, FSE 1997*, pages 149–165, 1997.

[DL08] Whitfield Diffie and George Ledin. SMS4 Encryption Algorithm for Wireless Networks. *IACR Cryptology ePrint Archive*, 2008:329, 2008.

[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 *Advances in Cryptology - CRYPTO 2011*, 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*, pages 326–341, 2011.

[GR14] Kishan Chand Gupta and Indranil Ghosh Ray. On Constructions of Circulant MDS Matrices for Lightweight Cryptography. In *Information Security Practice and Experience, ISPEC 2014*, pages 564–576, 2014.

[GWG15] Zhiyuan Guo, Wenling Wu, and Si Gao. Constructing Lightweight Optimal Diffusion Primitives with Feistel Structure. In *Selected Areas in Cryptography, SAC 2015*, pages 352–372, 2015.

[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*, pages 433–450, 2014.

[LBs+16] Ting Li, Jian Bai, Yao sun, Dingkang Wang, and Dongdai Lin. The Lightest $4 \times 4$ MDS Matrices over $GL(4, \mathbb{F}_2)$. *IACR Cryptology ePrint Archive*, 2016:686, 2016.

[LS16] Meicheng Liu and Siang Meng Sim. Lightweight MDS Generalized Circulant Matrices. In *Fast Software Encryption, FSE 2016*, pages 101–120, 2016.

[LW16] Yongqiang Li and Mingsheng Wang. On the Construction of Lightweight Circulant Involutory MDS Matrices. In *Fast Software Encryption, FSE 2016*, pages 121–139, 2016.

[MS77] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error Correcting Codes*. North-Holland Publishing Company, 1977.

[SDMO12] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Behnaz Omoomi. On Construction of Involutory MDS Matrices from Vandermonde Matrices in $GF(2^q)$. *Des. Codes Cryptography*, 64(3):287–308, 2012.

[SDMS12] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Pouyan Sepehrdad. Recursive Diffusion Layers for Block Ciphers and Hash Functions. In *Fast Software Encryption, FSE 2012*, pages 385–401, 2012.

[SKOP15] Siang Meng Sim, Khoongming Khoo, Frédérique E. Oggier, and Thomas Peyrin. Lightweight MDS Involution Matrices. In *Fast Software Encryption, FSE 2015*, pages 471–493, 2015.

[SS16] Sumanta Sarkar and Habeeb Syed. Lightweight Diffusion Layer: Importance of Toeplitz Matrices. *IACR Cryptology ePrint Archive*, 2016:835, 2016.

[WWW12] Shengbao Wu, Mingsheng Wang, and Wenling Wu. Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions. In *Selected Areas in Cryptography, SAC 2012*, pages 355–371, 2012.

[WZY15] Wenling Wu, Lei Zhang, and Xiaoli Yu. The DBlock Family of Block Ciphers. *SCIENCE CHINA Information Sciences*, 58(3):1–14, 2015.

[ZWFS09] Wentao Zhang, Wenling Wu, Dengguo Feng, and Bozhan Su. Some New Observations on the SMS4 Block Cipher in the Chinese WAPI Standard. In *Information Security Practice and Experience, ISPEC 2009*, pages 324–335, 2009.

# A Possible Forms of Rotational-XOR MDS Matrices

To facilitate the description, we illustrate the four block in the first row for each possible form in Figure 7.


**Figure 7:** The shapes of the first row in each of seven possible forms

# B Proof of Corollary 2

First, by using a similar method in Lemma 2, we obtain the statement below.

**Lemma 6.** *For an MDS* $Circ(A_1, \cdots, A_n)$*, if two consecutive blocks are identical, say* $A_1 = A_2$*, the sum of any other two consecutive blocks is non-singular.*

Next, we prove that if $M^{\mathcal{I}}_{n,b}$, $n > 4$, is a rotational-XOR MDS diffusion layer, then $|\mathcal{I}| \geq n + 2$.

*Proof.* It is obvious that $|\mathcal{I}| > n$, so we only need to prove that $M^{\mathcal{I}}_{n,b}$ is not MDS for $n > 4$ and $|\mathcal{I}| = n + 1$. Each row in $M^{\mathcal{I}}_{n,b}$ has exactly $n + 1$ 1's, so $n$ must be even for $M^{\mathcal{I}}_{n,b}$ to be invertible. In what follows, we consider the case of $n = 6$.

Due to the invertibility, there is at least one non-negative diagonal in each block. Since $|\mathcal{I}| = n + 1$, there is exactly one block with two non-negative diagonals. Similar to the discussion in the case of $n = 4$, such block is always the first block in the first row. Note that there are only 7 possible shapes of the blocks in $M_{n,b}^{\mathcal{I}}$ (See Figure 8). We discuss all possible cases of the first row. There are some points that need to be taken into consideration for $M_{n,b}^{\mathcal{I}}$ to be MDS:

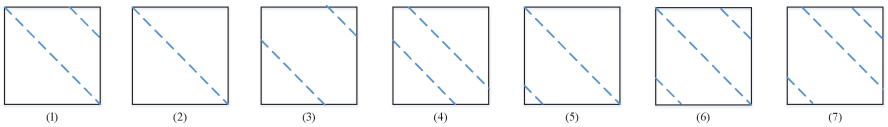


**Figure 8:** The possible shapes of blocks in $M_{n,b}^{\mathcal{I}}$ with $n > 4$ and $|\mathcal{I}| = n + 1$

(1) Based on our constraint, the first block can only be Figure 8-(1), Figure 8-(6), or Figure 8-(7). Then, any other block has exactly one non-negative diagonal, i.e. the other blocks are Figure 8-(2), Figure 8-(3), Figure 8-(4), Figure 8-(5).

(2) Each negative diagonal is from the previous block. Once the identity matrix (Figure 8-(2), which comes immediately after Figure 8-(5)) appears, all subsequent blocks, if any, are identity matrices. However, according to the discussion right above Section 4, the identity matrix should not occur in an MDS $M_{n,b}^{\mathcal{I}}$ with $|\mathcal{I}| = n + 1$;

(3) There is at most one block in the form of Figure 8-(4). If Figure 8-(4) does not appear, the four middle blocks become identical, which is a contradiction. So Figure 8-(4) occurs exactly once and must be in the third or fourth place (otherwise there are still 3 identical blocks).

(4) The last block should be either Figure 8-(5) or Figure 8-(3), and accordingly the first block is Figure 8-(1) or Figure 8-(6) (or Figure 8-(7)).

As a consequence, only three cases are left:

(a) Figure 8-(4) appears in the third place. Here the fourth and fifth blocks are identical. Meanwhile, the last block is Figure 8-(5), and the first block is Figure 8-(1). The sum of these two blocks is singular, which is a contradiction according to Lemma 6.

(b) Figure 8-(4) occurs in the fourth place and the last block is Figure 8-(3). Here the second block and third block are identical, and the first block is Figure 8-(6). Since the sum of the last two blocks (they are identical) is singular, this case is excluded.

(c) Figure 8-(4) appears in the fourth place and the last block is Figure 8-(5). Similar to the analysis in (a), this case is ruled out.

The discussion above is for $n = 6$, nevertheless, for other cases, it is even more true since more blocks are repeated. To summarize, any rotational-XOR MDS diffusion layer $M_{n,b}^{\mathcal{I}}$ with $n > 4$ must satisfy $|\mathcal{I}| \geq n + 2$. □