Lightweight MDS Generalized Circulant Matrices (Full Version)

Meicheng Liu[1,⋆] and Siang Meng Sim[2,⋆⋆]

[1] Nanyang Technological University, Singapore and State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, P. R. China
[2] Nanyang Technological University, Singapore
meicheng.liu@gmail.com, ssim011@e.ntu.edu.sg

Abstract. In this article, we analyze the circulant structure of generalized circulant matrices to reduce the search space for finding lightweight MDS matrices. We first show that the implementation of circulant matrices can be serialized and can achieve similar area requirement and clock cycle performance as a serial-based implementation. By proving many new properties and equivalence classes for circulant matrices, we greatly reduce the search space for finding lightweight maximum distance separable (MDS) circulant matrices. We also generalize the circulant structure and propose a new class of matrices, called *cyclic matrices*, which preserve the benefits of circulant matrices and, in addition, have the potential of being self-invertible. In this new class of matrices, we obtain not only the MDS matrices with the least XOR gates requirement for dimensions from 3×3 to 8×8 in $\mathrm{GF}(2^4)$ and $\mathrm{GF}(2^8)$, but also involutory MDS matrices which was proven to be non-existence in the class of circulant matrices. To the best of our knowledge, the latter matrices are the first of its kind, which have a similar matrix structure as circulant matrices and are involutory and MDS simultaneously. Compared to the existing best known lightweight matrices, our new candidates either outperform or match them in terms of XOR gates required for a hardware implementation. Notably, our work is generic and independent of the metric for lightweight. Hence, our work is applicable for improving the search for efficient circulant matrices under other metrics besides XOR gates.

Key words: lightweight cryptography, diffusion layer, MDS, circulant matrices.

1 Introduction

In the designing of symmetric-key ciphers, there are two fundamental concepts required for the overall security of the cipher—the confusion and diffusion prop-

[⋆] Supported by the National Natural Science Foundation of China (61303258, 61379139 and 11526215) and the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06010701.

[⋆⋆] Supported by the Singapore National Research Foundation Fellowship 2012 (NRF-NRFF2012-06).

erties described by Shannon [20]. Informally, the latter is to spread the internal dependencies as much as possible [21]. The diffusion layer of a cipher is often achieved by a linear diffusion matrix that transforms an input vector to some output vector through linear operations. For the choice of the diffusion layer, there can be a trade-off between the security and computation efficiency. Several designs compromise the diffusion power for a faster diffusion layer, while another trend is to maximize the diffusion power with *maximum distance separable* (MDS) matrices. The diffusion power of a matrix is often quantified by the branch number of the matrix, and an MDS matrix achieves maximum branch number, also known as perfect diffusion property. MDS matrices are widely used in many ciphers like AES [9], LED [11], SQUARE [8]. However, very often the price for having strong diffusion property is the heavy implementation cost, in either software or hardware implementations. Therefore, there is a need to reduce the implementation cost when perfect diffusion property is desired.

Recently, the designing and improving of hardware efficiency become a major trend. Several lightweight block ciphers [5,11,7,23] and lightweight hash functions [2,6,10] are designed to minimize the implementation cost. Notably in the hash function PHOTON [10], a new type of MDS matrices that can be computed recursively were proposed, so-called *serial matrices*, where a serial matrix A of order k is raised to power k and the resultant matrix A^k is MDS. In comparison to round-based implementation, serial-based implementation trades more clock cycles for lesser hardware area requirement. Such matrices were later used in block ciphers like LED [11] and more recently in authentication encryption scheme like the PRIMATEs [1].

In a nutshell, a round-based implementation computes the entire diffusion matrix of order k and applies the diffusion layer in one clock cycle. Hence, it is necessary to have all, if not most, of the k^2 entries of the diffusion matrix to be lightweight. On the other hand, a serial-based implementation computes the non-trivial row of a serial matrix[1], and applies it for k times recursively. Therefore, the primary implementation cost is the k entries of the non-trivial row and the computation time takes k clock cycles. Although it is natural to perceive that these two implementations require very different matrices, there are a type of matrices that can achieve the best of both worlds—circulant matrices.

Circulant matrices are a common type of matrices for the diffusion layer, a typical example of which is the AES diffusion matrix. They have a simple structure that every row is a right-shift of the previous row. Hence, a circulant matrix can be defined by its first row of k entries. In addition, it is known that an MDS circulant matrix can contain repeated lightweight entries. For instance in the AES diffusion matrix, there are two 1's which practically has no implementation cost for multiplication. In comparison to Hadamard matrices, another common type of matrices for the diffusion layer [3,4], which must contain k distinct entries to be MDS, circulant matrices tend to achieve lower implementation cost in a round-based implementation. Although circulant matrices cannot be directly used in

[1] A serial matrix of order k consists of $k-1$ rows with a single 1 and $k-1$ many 0's and a row with non-trivial entries.

a serial-based implementation, their circulant structure can be implemented in a serialized manner and achieve similar performance as the serial-based implementation. In short, using a circulant matrix in the diffusion layer gives the flexibility to do a trade-off between the area requirement and the clock cycle, whereas most of the other matrix types are suitable for either one but not both implementations.

One approach to build lightweight MDS matrices from some matrix type is to focus on some subclass of such matrices that are MDS, based on some predefined metric for lightweight, then pick the lightest MDS matrices from this subclass. In [16,13], the authors chose to maximise the number of 1's for better efficiency and constructed circulant-like matrices that are MDS with as many 1's as possible, then searched for the lightest MDS circulant-like matrices. In another work [12], the authors quantified lightweight with low Hamming weight and focused on involutory (self-inverse) matrices, they proposed the construction of Hadamard-Cauchy matrices that are MDS and can be involutory, then minimized the Hamming weight of a few entries of the Hadamard-Cauchy matrices. Although this approach is efficient for finding lightweight MDS matrices, the matrices found are optimal among the subclasses rather than the whole population of the matrix type.

Another approach is to pick the lightest matrix from some matrix type and check for MDS, and extend the search to the next lightest matrix if it is not MDS. This approach, also often regarded as exhaustive search, can be seen in [17,21]. The clear advantage of the exhaustive search over the previous approach is that it guarantees optimal for the given matrix type. In addition, it has the freedom to change the metric for lightweight when necessary. Despite the advantages, this approach suffers from the large search space. In [21], the authors tackled this problem by introducing the concept of the equivalence classes of Hadamard matrices to significantly reduce the search space for finding lightweight involutory MDS (IMDS) matrices. However, the equivalence relation for circulant matrices has not yet been discovered in the literatures.

There are two main challenges in the second approach. Given a set of lightweight coefficients, the first challenge in finding MDS circulant matrices with these coefficients would be the large search space due to the necessity of checking the MDS property for all possible permutations. The second challenge is that MDS circulant matrices can have repeated entries which makes the search space larger than other types of matrices, for instance Hadamard matrices, of the same order. Perhaps due to these challenges, the existing work on circulant matrix used either the first approach to find lightweight MDS circulant matrix of order 8 from some subclass of circulant matrices [13,14], or the second approach but could not complete the search for lightweight MDS circulant matrix of order 8 [17]. Therefore, this paper is devoted to tackle these problems and reduce the search space for finding generic lightweight MDS circulant matrices through analyzing the circulant structure.

Contributions. In Section 2.3, we illustrate how circulant matrices can have a trade-off between the area requirement and clock cycle in hardware implementation. This shows that using circulant matrix in a diffusion layer gives the designer the flexibility to choose the implementation between lower area requirement and faster computation according to the needs. In Section 3, we tackle both challenges faced when using the second approach for finding lightweight MDS circulant matrices. In Section 3.1, we prove the existence of equivalence classes for circulant matrices in terms of the branch number. Since the circulant matrices within an equivalence class have the same branch number, it is sufficient to check one representative from each equivalence class and hence reduce the search space. In Section 3.2, we show that there are at most 5 types of MDS circulant matrices for order $k \leq 8$, namely circulant matrices whose first row has k distinct entries, 1, 2 or 3 pairs of repeated entries, or 3 repeated entries. This allows us to complete the search for lightweight MDS circulant matrix of order 8 which previously was not achievable by [17]. In Section 4, we generalize the circulant structure and propose a new type of matrices—cyclic matrices, which preserve the benefits and advantages of circulant matrices. Using group theory, we prove that, in terms of branch number, cyclic matrices are equivalent to circulant matrices. This greatly simplifies the understanding and analysis on the branch number of the cyclic matrices. In Section 5, we present the lightest MDS left-circulant matrices (where each row is a left rotation instead of right), for order $k \leq 8$, based on the same metric used in [17,21]. In addition, we overcome the constraint that circulant matrix cannot be involutory and MDS simultaneously, and also present the lightest involutory MDS left-circulant matrices. To the best of our knowledge, the latter matrices are the first of its kind. We would like to emphasize that all the techniques and most results presented in this paper are independent of the metric for lightweight. In other words, one can choose another metric and apply our techniques to reduce the search space for finding the desired matrices.

2 Preliminary

In this section, we first state some notations that will be frequently used for the rest of the paper. Next, we formally define what branch number of a matrix is, and provide two propositions that will be useful in the later proofs. Lastly, we give an introduction to circulant matrix, the advantages of using it and how the implementation of circulant matrix can be serialized. In this paper, we assume that the matrices are square matrices unless otherwise stated.

2.1 Notations

n : Dimension of the finite field
$\mathrm{GF}(2^n)$: Finite field of order 2^n
`0x` : Prefix for hexadecimal, common notation for expressing binary polynomial coefficients or n-bit strings
k : Order of the square matrix
$M[i,j]$: (i,j)-entry of the matrix M, where $i, j \in \{0, 1, ..., k-1\}$
$wt(v)$: Number of nonzero components of the vector v

2.2 Branch number of the diffusion layer

Recall that the diffusion power of the diffusion layer is often quantified by the branch number of the diffusion matrix.

Definition 1. *The branch number of a matrix M of order k over finite field $\mathrm{GF}(2^n)$ is the minimum number of nonzero components in the input vector v and output vector $u = M \cdot v$ as we range over all nonzero $v \in [\mathrm{GF}(2^n)]^k$. I.e., the branching number of matrix M is $\mathcal{B}_M = \min_{v \neq 0}\{wt(v) + wt(Mv)\}$.*

That is to say, for any nonzero input and output pair of a diffusion matrix, the number of nonzero components will be at least the branch number of the diffusion matrix. This is essential for protecting against the cryptanalysis like differential attack that exploits the differential patterns between the plaintext and the ciphertext. As the sum of nonzero components is lower bounded by the branch number, having a high branch number implies that a small input difference will inevitably lead to a large output difference, and to achieve a small output difference would require a large input difference.

Definition 2. *[22] A maximum distance separable (MDS) matrix of order k is a matrix that attains the optimal branch number $k + 1$.*

When there is a single difference in the input vector, the best possible diffusion is to spread the difference to all k components of the output vector, hence the largest possible branch number is $k+1$. For instance, the `AES` diffusion matrix has order 4 and a branch number 5, hence it is MDS.

The following propositions are simple yet crucial building blocks for the results in this paper.

Proposition 1. *[18, Page 321, Th. 8] A matrix is MDS if and only if its square submatrices are all nonsingular.*

Proposition 2. *For any permutation matrices P and Q, the branch numbers of these two matrices M and PMQ are the same.*

Proof. Since P and Q are permutation matrices, there can be bijection mappings between the input vectors (resp. output vectors) of M and PMQ where the vectors differ by some permutation, hence the minimum number of nonzero components in the input and output pairs remains the same and they have the same branch number. □

2.3 Circulant matrices and its implementation

Circulant matrices. Here, let us formally define circulant matrices and related notations.

Definition 3. *A circulant matrix C of order k is a matrix where each subsequent row is a right rotation of the previous row. We denote the matrix as* $\mathrm{circ}(c_0, c_1, ..., c_{k-1})$*, where c_i's are the entries of the first row of the matrix. The (i, j)-entry of C can be expressed as $C[i, j] = c_{(j-i) \ mod \ k}$.*

There are several advantages of using circulant matrix in a diffusion layer:

1. It has a higher probability of finding an MDS matrix as compared to a randomized square matrix [8].
2. It has at most k distinct entries, and in addition it can be MDS and contain repeated lightweight entries, which tends to have lower implementation cost as compared to matrices like Hadamard and Cauchy matrices that must have at least k distinct entries in order to be MDS.
3. It has the flexibility to be implemented in both round-based and serialized implementations.

However, it was shown in [15] that involutory MDS (IMDS) circulant matrices of order 4 do not exist, and was further proved in [13] that IMDS circulant matrices of any order do not exist. To preserve the benefits of circulant matrices, we generalize the circulant structure in Section 4 and find lightweight IMDS matrices that are presented in Section 5.

Serialized implementation of circulant matrices. First, let us illustrate the round-based implementation using an arbitrary circulant matrix $\mathrm{circ}(a, b, c, d)$ of order 4, and an arbitrary input vector (w, x, y, z), we compute the output vector as follows,

$$\begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix} \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} aw + bx + cy + dz \\ dw + ax + by + cz \\ cw + dx + ay + bz \\ bw + cx + dy + az \end{pmatrix}.$$

The entire diffusion matrix is implemented and the output components can be computed in parallel and in one clock cycle.

On the other hand, one clock cycle of a serial-based implementation is computed as follows,

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a & b & c & d \end{pmatrix} \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \\ aw + bx + cy + dz \end{pmatrix},$$

where the output is fed back to the input and this process is repeated for another 3 times to get the final output. Excluding the control logics and memories required, serial-based implementation requires implementing one row of the matrix and takes k clock cycles to compute the output vector.

Clearly a circulant matrix can be implemented in the round-based manner. Although it is not in a form of a serial matrix that is required for serial-based implementation, implementation of a circulant matrix can still be serialized. The key observation is that the same permutation is applied to obtain each subsequent row. For a circulant matrix, the permutation is a right rotation. To serialize the implementation of circulant matrix, we implement the first row of the circulant matrix and compute the first output component.

$$\begin{pmatrix} a\ b\ c\ d \\ \\ \\ \\ \end{pmatrix} \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} aw + bx + cy + dz \\ \\ \\ \\ \end{pmatrix}.$$

Next, we update the input vector by applying the inverse permutation to obtain (x, y, z, w) and apply the first row of the matrix again,

$$\begin{pmatrix} a\ b\ c\ d \\ \\ \\ \\ \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} \\ ax + by + cz + dw \\ \\ \\ \end{pmatrix},$$

and we obtain the second component of the output vector. We repeat the process to obtain the entire output vector in 4 clock cycles. Thus, similar to serial-based implementation, we only need to implement one row of the matrix and it takes k clock cycles to compute the output vector.

In fact, one can even achieve other area requirement and clock cycle trade-offs that are between the round-based and serial-based implementation performance. In the previous example, one can also implement 2 rows of the circulant matrix and compute 2 output components in parallel, this will take 2 clock cycles to complete the diffusion layer computation. More generally, we can have t-serialized implementation when we are using circulant matrices, where t divides k. The estimated implementation costs and clock cycles required for the implementations are summarized in Table 1. Note that this does not include the memory costs and control logics required for different implementations. From Table 1, it is clear that the round-based and serialized implementations are special case of t-serialized implementation where $t = 1$ and $t = k$ respectively.

Table 1. Estimated implementation costs and clock cycles for various implementations

Type of Implementation	Matrix Implementation (No. of entries)	Clock Cycle
Round-based	k^2	1
Serial-based	k	k
Serialized	k	k
t-serialized	k^2/t	t

Circulant matrices are not the only matrix type that can be serialized. In fact, if the same permutation, not necessarily being a right rotation, is applied to obtain each subsequent row, we can still serialize the implementation. This observation leads us to generalize the circulant matrices to cyclic matrices, see also Section 4, which can be serialized too.

3 Properties of Circulant Matrices

There are mainly two challenges in the method of picking the lightest circulant matrix and checking the MDS property. Firstly, for a generic (not considering the values of the entries) circulant matrix of order k, $\mathrm{circ}(c_0, c_1, ..., c_{k-1})$, there are $k!$ ways to permute the entries, which can quickly be intractable. Secondly, the choice of the k lightweight nonzero entries need not be distinct, which potentially cause the search space to be much larger than just choosing k distinct entries and permuting them.

In Section 3.1, we first introduce an equivalence relation to partition the $k!$ circulant matrices into equivalence classes, where circulant matrices within an equivalence class share the same branch number. This allows us to reduce the search space by checking the MDS property for one representative from each equivalence class. Next in Section 3.2, we analyze the circulant structure and show that for order $k \leq 8$, there are at most 5 types of MDS circulant matrices, namely circulant matrices whose first row has k distinct entries, 1, 2 or 3 pairs of repeated entries, or 3 repeated entries. This shows that any MDS circulant matrix must belong to one of these 5 types.

3.1 Compact equivalence classes of circulant matrices

For the ease of our discussion on the permutation of the entries, we focus on the permutation of the index of the elements.

Definition 4. *An index permutation σ on an ordered set $\{c_0, c_1, ..., c_{k-1}\}$ is a permutation that permutes the index of the elements.*

Example 1. Let σ be an index permutation on an ordered set $\{c_0, c_1, c_2, c_3, c_4\}$ where $\sigma(i) = 4 - i$, the resultant ordered set will be $\{c_4, c_3, c_2, c_1, c_0\}$.

Definition 5. *Given a matrix M of order k that is defined by its first row under a rule, we denote by M^σ the matrix generated under the same rule by the first row of M modified by applying an index permutation σ.*

Definition 6. *Two matrices M and M' are called permutation-equivalent, denoted by $M \sim_{\mathcal{B}} M'$, if there exist two permutation matrices P and Q such that $M' = PMQ$.*

It is easy to verify that $\sim_{\mathcal{B}}$ is a well-defined equivalence relation. By Proposition 2, we know that the permutation-equivalent matrices have the same branch number. Using this equivalence relation, we partition the $k!$ possible circulant matrices into equivalence classes with respect to their branch number.

Definition 7. *An equivalence class of circulant matrices is a set of circulant matrices satisfying the equivalence relation $\sim_{\mathcal{B}}$.*

We first analyze what index permutation satisfies the relation, then we deduce the number of equivalence classes of circulant matrices.

Lemma 1. *Given two circulant matrices C and C^{σ}, $C \sim_{\mathcal{B}} C^{\sigma}$ if and only if σ is some index permutation satisfying $\sigma(i) = (bi + a) \bmod k$, $\forall i \in \{0, 1, ..., k-1\}$, where $a, b \in \mathbb{Z}_k$ and $\gcd(b, k) = 1$.*

Proof. The "if" direction is immediate once we have proven the "only if" direction. Assume that $C \sim_{\mathcal{B}} C^{\sigma}$. By Definition 6, there exists permutation matrices P and Q such that $C^{\sigma} = PCQ$, where P (resp. Q) is in fact a row (resp. column) permutation on C. Since C is circulant, one can observe that if $C^{\sigma} = PC$, then the first row of C^{σ} is some row of C and thus corresponds to some rotation of the first row of C, which shows that the index permutation σ can be expressed as $\pi_a(i) = (i + a) \bmod k$. That is, π_a corresponds to a row permutation P_a. Therefore, for any C^{σ} such that $C^{\sigma} = PCQ$, we can always apply some index permutation π_{-a} to fix the first element c_0 and accordingly pre-multiply C^{σ} by a corresponding row permutation P_{-a}, which gives $C^{\pi_{-a} \circ \sigma} = P_{-a}PCQ$, where $\pi_{-a}(\sigma(0)) = 0$.

Next, we consider index permutation that fixes 0. Note that this implies that the row and column permutations on C fix the first row and column. Suppose that $C^{\phi_b} = PCQ$, $\phi_b(0) = 0$ and $\phi_b(1) = b$, then the column permutation Q maps column b of C to column 1 of C^{ϕ_b}, and similarly the row permutation P maps row $k - b$ of C to row $k - 1$ of C^{ϕ_b}. By definition of circulant matrices, we know that $c_{\phi_b(2)}$, which is the third entry of C^{ϕ_b}, can be written as $C^{\phi_b}[0, 2] = C^{\phi_b}[(k-1), 1]$. Since the pre-image of row $k-1$ and column 1 of C^{ϕ_b} are row $k-b$ and column b of C, we can express that entry of C^{ϕ_b} as an entry of C, that is $C^{\phi_b}[(k-1), 1] = C[(k-b), b]$. And again by definition of circulant matrices, the entry $c_{b-(k-b) \bmod k} = c_{2b \bmod k}$. That is to say, by defining $\phi_b(1) = b$, we have restricted the permutation of the next index to be $\phi_b(2) = 2b \bmod k$. Following the same argument, we can conclude that $\phi_b(i) = bi \bmod k$. In addition, we must have $\gcd(b, k) = 1$ so that ϕ_b is a permutation on $\{0, 1, ..., k-1\}$.

Finally, we can see that if $C \sim_{\mathcal{B}} C^{\sigma}$ then $\sigma = \pi_a \circ \phi_b$, that is, $\sigma(i) = (bi + a) \bmod k$. □

For simplicity, we call the permutations satisfying Lemma 1 the $\mathcal{C}$-permutations. That is to say, $C \sim_{\mathcal{B}} C^{\sigma}$ if and only if σ is a $\mathcal{C}$-permutation. We show in Appendix A how to generate one representative for each equivalence class.

Theorem 1. *There are $\frac{(k-1)!}{\varphi(k)}$ equivalence classes of circulant matrices of order k, where $\varphi(k)$ is the Euler's totient function.*

Proof. It is clear that the cardinality of each equivalence class is the number of possible index permutation σ. By Lemma 1, we know that $\sigma(i) = (bi + a) \bmod$

k, where $a, b \in \mathbb{Z}_k$ and $\gcd(b, k) = 1$. Since there are k possible values for a and b has to be coprime with k, there are $\varphi(k)$ possible values for b, and each equivalence class has cardinality of $k \cdot \varphi(k)$. Hence the number of equivalence classes is $\frac{k!}{k \cdot \varphi(k)} = \frac{(k-1)!}{\varphi(k)}$. □

Note that the "only if" direction of the Lemma 1 implies that this is the most compact equivalence classes for generic circulant matrices in terms of branch number. In [21], the authors presented equivalence classes of Hadamard matrices to reduce the search space for checking the MDS property. But whether there exists larger (more compact) equivalence classes to further reduce the search space remains an open question. Observing its similarity with our work, we analyze the equivalence classes of Hadamard matrices in [21] and find that it is already the most compact equivalence class. We present the proof in Appendix B for readers who are interested in the equivalence classes of Hadamard matrices.

3.2 Types of MDS circulant matrices of order $k \leq 8$

In short, this section proves the following theorem.

Theorem 2. *For order $k \leq 8$, there are at most 5 types of MDS circulant matrices, namely circulant matrices whose first row has:*

Type 0: *k distinct entries;*
Type 1: *1 pair of repeated entries;*
Type 2: *2 pairs of repeated entries;*
Type 3: *3 pairs of repeated entries;*
Type 4: *or 3 repeated entries.*

Given an ordered multi-set of entries $\{c_0, c_1, ..., c_{k-1}\}$, suppose that two entries of them are the same, denoted by $c_i = c_{(i+d) \bmod k}$ for some $i, d \in \{0, 1, ..., k-1\}$. From Section 3.1, we see that any rotation of the entries are permutation-equivalent. Hence, for any $d > \lfloor \frac{k}{2} \rfloor$, it is equivalent to considering $c_{(i-d) \bmod k} = c_{(i-d)+d}$ which is equal to $c_{i+(k-d) \bmod k} = c_i$, where $k - d \leq \lfloor \frac{k}{2} \rfloor$. Without loss of generality, we assume $i + d \leq k - 1$ and $d \leq \lfloor \frac{k}{2} \rfloor$.

First, we state two lemmas that will help us in proving Theorem 2.

Lemma 2. *An MDS circulant matrix of even order k does not have $c_i = c_{i+\frac{k}{2}}$.*

Proof. Suppose that there exists $c_i = c_{i+\frac{k}{2}}$. Considering the submatrix of order 2 by taking row 0 and $\frac{k}{2}$, and column i and $i + \frac{k}{2}$, we have

$$\begin{pmatrix} c_i & c_{i+\frac{k}{2}} \\ c_{(i-\frac{k}{2}) \bmod k} & c_i \end{pmatrix}.$$

Since $i - \frac{k}{2} \equiv i + \frac{k}{2} \pmod{k}$, we have a singular submatrix and by Proposition 1, there is a contradiction. □

Lemma 3. *An MDS circulant matrix does not have $c_i = c_{i+d}$ and $c_j = c_{j+d}$, where $i \neq j$.*

Proof. Suppose that there exist $c_i = c_{i+d}$ and $c_j = c_{j+d}$, where $i < j$. Consider the submatrix of order 2 by taking row 0 and $(i - j) \bmod k$, and column i and $i + d$, we have

$$\begin{pmatrix} c_i & c_{i+d} \\ c_j & c_{j+d} \end{pmatrix},$$

Since these two columns are identical, we have a singular submatrix and by Proposition 1, there is a contradiction. □

From Lemma 2 and 3, we can conclude that an MDS circulant matrix of order k allows at most $\lfloor \frac{k-1}{2} \rfloor$ possible distinct distances and thus has at least $\lceil \frac{k+1}{2} \rceil$ distinct elements. Specially for order $k = 8$, it allows 3 possible distinct distances and thus there are at most 3 pairs of repeated entries. If some entry has multiplicity 3, say $c_i = c_{i+d_1} = c_{i+d_2}$, then the three distances $d_1, d_2, d_2 - d_1$ are pairwise distinct. It also implies that any higher multiplicity is impossible for an MDS circulant matrix of order 8 as the number of pairwise equalities is more than 3 (a similar property that an MDS matrix of order 8 has at most 24 ones was proved in [16]). Similarly, for order $k < 8$, there are also at most 3 possible distances. Therefore, we obtain Theorem 2 that any MDS circulant matrix of order $k \leq 8$ is one of the 5 matrix types.

Table 2. Possible types of MDS circulant matrices of order $k \leq 8$

Order	Possible d	k distinct	1 pair	2 pairs	3 pairs	3 repeated
3	$\{1\}$	✓	✓			
4	$\{1\}$	✓	✓			
5	$\{1, 2\}$	✓	✓	✓		
6	$\{1, 2\}$	✓	✓	✓		
7	$\{1, 2, 3\}$	✓	✓	✓	✓	✓
8	$\{1, 2, 3\}$	✓	✓	✓	✓	✓

In Table 2, we list all the possible types of MDS circulant matrices for order $k \leq 8$. These results can also be extended to higher order circulant matrices. Note that this is a necessary condition for an MDS circulant matrix, it does not guarantee the existence of MDS circulant matrix for any of the circulant matrix type. For $k = 8$, we check that there are MDS matrices of each type, see also Section 5.

4 Cyclic Matrices

In this section, we generalize the circulant matrix structure and introduce a new type of matrices, we call them the *cyclic matrices*. Despite that cyclic matrices capture the essential requirement to have t-serialized implementation, analyzing all cyclic matrices is not feasible. Using results from elementary group theory, we can relate cyclic matrices to circulant matrices in terms of branch number. This allows us to apply the results on circulant matrices in Section 3 to the cyclic matrices as well.

Generalized circulant matrices. Recall from Section 2.3 that to serialize the implementation of a matrix, the same permutation is applied to obtain each subsequent row. Hence, we generalize the circulant structure by considering other permutations beside the right rotation.

Definition 8. *A cyclic matrix C_ρ of order k is a matrix where each subsequent row is some permutation ρ of the previous row, where ρ is a cycle of length k. We denote the matrix as $\mathrm{cyc}_\rho(c_0, c_1, ..., c_{k-1})$, where c_i's are the entries of the first row of the matrix. The (i, j)-entry of C_ρ can be expressed as $C_\rho[i, j] = c_{\rho^i(j)}$.*

For example, the permutation of the circulant matrix structure can be expressed as a cycle $(0\ \ 1\ \ 2\ ...\ k-1)$, where $\rho = (i_0\ \ i_1\ \ i_2\ ...\ i_{k-1})$ means $\rho(i_j) = i_{(j-1) \bmod k}$ for $0 \le j \le k-1$. In the definition of cyclic matrix, we require the permutation to be a cycle of length k to avoid repeated rows and repeating elements in a column (which will not satisfy the property of MDS).

Since there are $(k-1)!$ cycles of length k, it is infeasible to analyze every single the cyclic structures. However, using Proposition 2 and elementary group theory, we can elegantly reduce the problem to simply analyzing the circulant matrices. First, observe that the permutation ρ is an element of the symmetric group S_k, and the collection of the permutations of the k rows of the matrix forms a cyclic group, hence the name cyclic matrices.

Example 2. Considering the cycle permutation $\rho = (0\ \ 2\ \ 1\ \ 3)$, we can express $\mathrm{cyc}_\rho(a, b, c, d)$ as follows

$$\begin{pmatrix} (a,b,c,d) \\ \rho(a,b,c,d) \\ \rho^2(a,b,c,d) \\ \rho^3(a,b,c,d) \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ d & c & a & b \\ b & a & d & c \\ c & d & b & a \end{pmatrix},$$

where the collection of the permutations of each row forms a cyclic group of order 4, $\langle(0\ \ 2\ \ 1\ \ 3)\rangle = \{(), (0\ \ 2\ \ 1\ \ 3), (0\ \ 1)(2\ \ 3), (0\ \ 3\ \ 1\ \ 2)\}$.

Relation to circulant matrices. Next, we show that any cyclic matrix is permutation-equivalent to some circulant matrix. More preciously, there is a bijection between the cyclic and circulant matrices satisfying $\sim_{\mathcal{B}}$. To prove this, we use the following proposition from elementary group theory.

Proposition 3. *[19, Ch. 5.3] Any two permutations ρ, τ which have the same cycle type are conjugate in S_k.*

That is to say, there exists permutation $\sigma \in S_k$ such that $\sigma\rho = \tau\sigma$. In the nutshell, σ can be computed by placing one permutation above the other and view it as a Cauchy's 2-line notation for permutation.

Example 3. Let $\rho = (0 \ \ 2 \ \ 1 \ \ 3)$ and $\tau = (0 \ \ 1 \ \ 2 \ \ 3)$, viewing it as a Cauchy's 2-line notation, we have

$$\begin{pmatrix} 0 & 2 & 1 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix},$$

from which we see that 0 and 3 are fixed while 1 and 2 are swapped. Therefore, we obtain $\sigma = (1 \ \ 2)$ and we can verify that $\sigma\rho = \tau\sigma$.

Theorem 3. *Given an ordered set S with k elements and some cyclic matrix structure, there exists a bijection between the cyclic matrices and the circulant matrices satisfying the relation $\sim_{\mathcal{B}}$, where both sets of matrices are generated by some index permutation on S.*

Proof. Let the permutation of some cyclic matrix be ρ and circulant matrix be $\tau = (0 \ \ 1 \ \ 2 \ \ ... \ \ k-1)$. By Proposition 3, there exist some permutation σ such that $\sigma\rho = \tau\sigma$. Hence for any row $i \in \{0, 1, ..., k-1\}$, we have $\sigma\rho^i = \tau^i\sigma$. In the form of a matrix, the permutation for each row of the matrices can be expressed as

$$\begin{pmatrix} \sigma(S) \\ \sigma \circ \rho(S) \\ \sigma \circ \rho^2(S) \\ \vdots \\ \sigma \circ \rho^{k-1}(S) \end{pmatrix} = \begin{pmatrix} \sigma(S) \\ \tau \circ \sigma(S) \\ \tau^2 \circ \sigma(S) \\ \vdots \\ \tau^{k-1} \circ \sigma(S) \end{pmatrix},$$

where σ in the cyclic matrix can be viewed as a column permutation, while in the circulant matrix it is a index permutation on S. Therefore by Proposition 2, the cyclic matrix has the same branch number as a circulant matrix that undergoes index permutation σ.

Lastly, one can easily infer that for any index permutation π on the cyclic matrix, it corresponds to a circulant matrix that undergoes index permutation $\sigma \circ \pi$. □

Example 4. Consider a cyclic matrix of order 4 with the row permutation $\rho = (0 \ \ 2 \ \ 1 \ \ 3)$, while the circulant matrix is $\tau = (0 \ \ 1 \ \ 2 \ \ 3)$. From Example 3, we have $\sigma = (1 \ \ 2)$ that satisfies $\sigma\rho = \tau\sigma$. Applying column permutation σ on the cyclic matrix and index permutation σ on circulant matrix, we obtain the same matrix as follows

$$\begin{pmatrix} a & b & c & d \\ d & c & a & b \\ b & a & d & c \\ c & d & b & a \end{pmatrix} \xrightarrow{\text{col perm } \sigma} \begin{pmatrix} a & c & b & d \\ d & a & c & b \\ b & d & a & c \\ c & b & d & a \end{pmatrix} \xleftarrow{\text{index perm } \sigma} \begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}.$$

This theorem shows that for any cyclic matrix, we have some column permutation σ that transforms it into a circulant matrix (or any other cyclic matrix) while preserving the branch number. However, the involution property of circulant matrix may not hold true for the cyclic matrices, which gives us an insight that there might exist IMDS cyclic matrices while it is not the case for the circulant matrices. And we indeed find IMDS cyclic matrices which are presented in Section 5.

Corollary 1. *Any cyclic matrix corresponds to some circulant matrix preserving the coefficients and the branch number.*

This is immediate from Theorem 3 and the fact that their entries are the same up to some permutation. In addition, we can draw the following corollary immediately from Theorem 2 and 3.

Corollary 2. *For order $k \leq 8$, there are at most 5 types of MDS cyclic matrices, namely cyclic matrices whose first row has:*

Type 0: *k distinct entries;*
Type 1: *1 pair of repeated entries;*
Type 2: *2 pairs of repeated entries;*
Type 3: *3 pairs of repeated entries;*
Type 4: *or 3 repeated entries.*

5 Results on Lightest (Involutory) MDS Matrices

There are different ways to define lightweight/efficient. For instance in AES, the diffusion matrix entries were chosen for its simplicity and low Hamming weight, while [16,14] defined efficiency by the number of 1's in the matrix. In hardware implementation, it is common to consider the area required and a simplified metric is to count the number of XOR gates needed for implementation. In [16,17,21], the authors evaluate the number of XOR gates needed to implement the multiplication of the diffusion matrices. Detailed description of the XOR count can be found in [16,17,21]. In this paper, we quantify the weight of a diffusion matrix by the sum of XOR counts in its first row[2].

In this section, we mainly focus on a special case of cyclic matrices, called left-circulant matrices. First, we provide a strategy to search for MDS left-circulant matrices by exploiting the properties of the matrices, including the permutation-equivalence relationship. Then, we show that, though no circulant matrices are IMDS, there are IMDS left-circulant matrices. We also provide a strategy to search for such IMDS matrices. The experimental results show that all the lightest MDS matrices and IMDS matrices can be confirmed for $3 \leq k \leq 8$, by using our strategies.

[2] This is adapted from [17], in which the number of XOR counts of one row is given by $\sum_{i=1}^{k} \gamma_i + (\ell - 1) \cdot n$, where γ_i is the XOR count of the i-th entry and ℓ is the number of nonzero coefficients in the row. Since the latter term is fixed for any MDS matrix of order k over $\mathrm{GF}(2^n)$, we are only interested in the sum of the XOR counts of the coefficients in a row.

5.1 Lightweight MDS left-circulant matrices

The definition of left-circulant matrices is given as follows.

Definition 9. *A left-circulant matrix L of order k is a matrix where each subsequent row is a left rotation of the previous row. We denote the matrix as $\ell\text{-circ}(c_0, c_1, ..., c_{k-1})$, where c_i's are the entries of the first row of the matrix. The (i, j)-entry of L can be expressed as $L[i, j] = c_{(i+j) \bmod k}$.*

It is infeasible to exhaust all the possible MDS left-circulant matrices over GF(2^8) for $k = 8$. Notice that the permutation-equivalence relationship (Lemma 1) of circulant matrices also applies to left-circulant matrices. Combining Corollary 2 and permutation-equivalence relationship, we can exhaust all the possible MDS left-circulant matrices over GF(2^n) with small XOR count for $n \leq 8$ and $k \leq 8$.

To efficiently determine whether a left-circulant matrix is MDS, we collect in advance the symbolic expressions of all determinants of its submatrices, and use them to compute the values of determinants. Once detecting that a determinant has value 0, the matrix is confirmed to be not MDS; otherwise, it is MDS. Using this method, the detection of MDS left-circulant matrices is speeded up (by dozens of times for $5 \leq k \leq 8$) since a lot of submatrices have the same determinants in terms of symbolic expressions.

Table 3. Lightest MDS left-circulant matrices of order $3 \leq k \leq 8$

k	Polynomial	Left-circulant matrices	XOR count
GF(2^8)			
3	0x1c3	(0x1, 0x1, 0x2)	3
4	0x1c3	(0x1, 0x1, 0x2, 0x91)	8
5	0x1c3	(0x1, 0x1, 0x2, 0x91, 0x2)	11
6	0x1c3	(0x1, 0x2, 0xe1, 0x91, 0x1, 0x8)	18
7	0x1c3	(0x1, 0x1, 0x91, 0x2, 0x4, 0x2, 0x91)	21
8	0x1c3	(0x1, 0x1, 0x2, 0xe1, 0x8, 0xe0, 0x1, 0xa9)	30
GF(2^4)			
3	0x13	(0x1, 0x1, 0x2)	1
4	0x13	(0x1, 0x1, 0x9, 0x4)	3
5	0x13	(0x2, 0x2, 0x9, 0x1, 0x9)	4
6	0x13	(0x1, 0x1, 0x9, 0xc, 0x9, 0x3)	12

We show in Table 3 our experimental results on MDS left-circulant $k \times k$ matrices over GF(2^n) with smallest XOR count for $n = 4, 8$ and $3 \leq k \leq 8$. All the provided matrices are optimal among the MDS cyclic matrices in terms of the metric as used in [17,21]. We also exhaust all the left-circulant matrices over GF(2^4) for $k = 7, 8$, and the results show that no such matrices are MDS. It was also noted in [17] that there do not exist circulant 8×8 matrices over GF(2^4).

We list in Table 4 the lightest 8×8 MDS matrices for each type of left-circulant matrices as well as the lightest ones under the two commonly used irreducible polynomials, 0x11b and 0x11d, which are respectively adopted in AES and WHIRLPOOL, and we compare them with the WHIRLPOOL matrix and the MDS Hadamard matrix found in [21]. From this table, we can see that the lightest MDS left-circulant matrices of all types except Type 0 (in which all the coefficients are distinct) have XOR count smaller than the known best ones. For WHIRLPOOL, we also provide an MDS left-circulant matrix which has smaller XOR count using the same irreducible polynomial as in WHIRLPOOL.

Table 4. Comparison of 8×8 MDS matrices

Type	Polynomial	Matrices	XOR count
4	0x1c3	(0x1, 0x1, 0x2, 0xe1, 0x8, 0xe0, 0x1, 0xa9)	30
3	0x1c3	(0x1, 0x1, 0x91, 0x2, 0x4, 0x2, 0x12, 0x91)	32
2	0x1c3	(0x1, 0x1, 0x4, 0x2, 0xa9, 0x91, 0x2, 0x3)	33
1	0x1c3	(0x1, 0x1, 0x2, 0xe0, 0x6, 0xe1, 0x91, 0x4)	35
0	0x1c3	(0x1, 0x2, 0x91, 0x8, 0x4, 0x6, 0xe1, 0x3)	42
4	0x11b	(0x1, 0x1, 0x2, 0x1, 0x74, 0x8d, 0x46, 0x4)	35
4	0x11d	(0x1, 0x1, 0x2, 0x8e, 0x47, 0x10, 0x1, 0x46)	34
4	0x11d	WHIRLPOOL	49
-	0x1c3	Hadamard [21]	40

We also compare in Table 5 our candidates with the previous lightweight MDS matrices for $n < 8$. It shows that all our candidates have the minimum XOR count, though some of them have the same XOR count as the known ones.

5.2 Lightweight IMDS left-circulant matrices

In this section, we first describe the involutory MDS left-circulant matrices and then show our experimental results.

Before showing our main results, we provide some useful properties for left-circulant matrices. It is known that the product of two circulant matrices is a circulant matrix. For left-circulant matrices, a similar property can be obtained. To simplify the presentation of the proofs, we omit "modulo k" from the indexes but it is expected that modulo k is applied when necessary.

Proposition 4. *The product of two left-circulant matrices is a circulant matrix.*

Proof. Let $A = \ell\text{-circ}(a_0, a_1, ..., a_{k-1})$ and $B = \ell\text{-circ}(b_0, b_1, ..., b_{k-1})$ be two left-circulant matrices. Then the (i, j)-entry of their product is $\sum_{t=0}^{k-1} A[i,t] \cdot B[t,j] = \sum_{t=0}^{k-1} a_{i+t} b_{t+j} = \sum_{t=0}^{k-1} a_t b_{t+(j-i)}$, which completes the proof. □

It is shown in [14] that $C^{2^d} = (\sum_{i=0}^{2^d-1} c_i)^{2^d} I$ and $\det(C) = (\sum_{i=0}^{2^d-1} c_i)^{2^d}$ for any $2^d \times 2^d$ circulant matrix $C = \text{circ}(c_0, c_1, ..., c_{2^d-1})$ over $\mathrm{GF}(2^n)$. Thus we have the following result for left-circulant matrices.

Table 5. Comparison of MDS matrices of order $k < 8$

k	Polynomial	Matrices	Matrix form	XOR count
GF(2^8)				
4	0x1c3	[21]	Hadamard	13
4	0x11d	[17]	serial/circulant	9
4	0x1c3	this paper	left-circulant	8
6	0x11b	PHOTON P_{288}	serial	23
6	0x1c3	this paper	left-circulant	18
GF(2^4)				
4	0x13	[21]	Hadamard	5
4	0x13	LED	serial	4
4	0x13	[17]	serial/circulant	3
4	0x13	this paper	left-circulant	3
5	0x13	PHOTON P_{100}	serial	4
5	0x13	this paper	left-circulant	4
6	0x13	PHOTON P_{144}	serial	14
6	0x13	this paper	left-circulant	12

Proposition 5. *For* $2^d \times 2^d$ *matrix* $L = \ell\text{-circ}(c_0, c_1, ..., c_{2^d-1})$ *over* $\mathrm{GF}(2^n)$, $L^{2^{d+1}} = (\sum_{i=0}^{2^d-1} c_i)^{2^{d+1}} I$ *and* $\det(L) = (\sum_{i=0}^{2^d-1} c_i)^{2^d}$.

Proof. By the proof of Propostion 4, we know L^2 is a circulant matrix with (i,j)-entry $\sum_{t=0}^{2^d-1} c_t c_{t+(j-i)}$, and thus $(L^2)^{2^d} = (\sum_{i=0}^{2^d-1} \sum_{t=0}^{2^d-1} c_t c_{t+i})^{2^d} I = ((\sum_{t=0}^{2^d-1} c_t)^2)^{2^d} I$, which also implies $\det(L) = (\sum_{i=0}^{2^d-1} c_i)^{2^d}$. □

Proposition 6. *For matrix* $L = \ell\text{-circ}(c_0, c_1, ..., c_{k-1})$ *over* $\mathrm{GF}(2^n)$, *L is involutory if and only if* $\sum_{i=0}^{k-1} c_i = 1$ *and* $\sum_{i=0}^{k-1} c_i c_{i+j} = 0$ *for all* $1 \le j \le \lfloor \frac{k-1}{2} \rfloor$.

Proof. Since the (i,j)-entry of L^2 is $\sum_{t=0}^{k-1} c_t c_{t+(j-i)}$, L is involutory if and only if $\sum_{t=0}^{k-1} c_t = 1$ and $\sum_{t=0}^{k-1} c_t c_{t+(j-i)} = 0$ for $j \neq i$. The proof is completed by the facts that $\sum_{t=0}^{k-1} c_t c_{t+(j-i)} = \sum_{t=0}^{k-1} c_t c_{t+(i-j)}$ and $\sum_{t=0}^{k-1} c_t c_{t+\frac{k}{2}} = 0$ for even k. □

A left-circulant matrix is symmetric and thus an involutory left-circulant matrix is orthogonal. It was shown in [14] that a circulant matrix is not IMDS and an orthogonal circulant $2^d \times 2^d$ matrix is not MDS. Similarly, we can prove that an involutory (orthogonal) left-circulant $2^d \times 2^d$ matrix is not MDS.

Theorem 4. *If L is a* $2^d \times 2^d$ *left-circulant matrix over* $\mathrm{GF}(2^n)$, *then L is not IMDS.*

Proof. It is sufficient to prove that if L is involutory then L is not MDS. Assume that $L = \ell\text{-circ}(c_0, c_1, ..., c_{2^d-1})$ is involutory. By Propostion 6, it holds that $\sum_{i=0}^{2^d-1} c_i c_{i+2t+1} = 0$ for $0 \le t \le 2^{d-2} - 1$, and thus $(\sum_{t=0}^{2^{d-1}-1} c_{2t})(\sum_{t=0}^{2^{d-1}-1} c_{2t+1}) = \sum_{t=0}^{2^{d-2}-1} \sum_{i=0}^{2^d-1} c_i c_{i+2t+1} = 0$. Note that

ℓ-circ$(c_0, c_2, ..., c_{2^d-2})$ and ℓ-circ$(c_1, c_3, ..., c_{2^d-1})$ are two submatrices of L. Therefore, according to Proposition 5, at least one of the determinants of these two submatrices equals 0, which shows L is not MDS. □

Our computations also show that there are no IMDS cyclic matrices for $k = 4, 8$. Nevertheless, there are IMDS left-circulant matrices for $k = 3, 5, 6, 7$.

Next we explain how to search for IMDS left-circulant matrices. Notice that an IMDS left-circulant matrix must satisfy the $\lfloor \frac{k+1}{2} \rfloor$ equations mentioned in Proposition 6. Theoretically, we can solve the equations and then check whether the solutions satisfy the MDS property. However, it is unclear how to efficiently solve the equations in a straightforward way. Solving the equations over GF(2^n) using Gröbner basis is very slow for $n = 8$ and is slow even for $n = 4$. To find the solutions faster, we first guess the values of about $\lfloor \frac{k-1}{2} \rfloor$ out of the k coefficients, then solve the equations. For $n = 4$, we guess all the possible values. For $n = 8$, we only guess some of the lightest elements. Our experiments show that it is sufficient to guess the lightest 9 elements to find the lightest IMDS left-circulant matrix.

We can check by Lemma 1 and Proposition 6 that if a left-circulant matrix is involutory then all its permutation-equivalent matrices are involutory. Thus we can use permutation-equivalence relationship to reduce the search space. In other words, once obtain an upper bound of the minimum XOR count, we can exhaust all the possible IMDS left-circulant matrices less than the threshold, and confirm the lightest one, as done for MDS left-circulant matrices.

We provide our results in Table 6. As shown in the table, there are no IMDS left-circulant matrices over GF(2^4) for $k = 6$. All the listed matrices have been confirmed to achieve the smallest XOR count.

Table 6. Lightest IMDS left-circulant matrices of order $3 \leq k \leq 7$

k	Polynomial	Matrices	XOR count
GF(2^8)			
3	0x169	(0x5a, 0xa, 0x51)	30
4	-		
5	0x165	(0x1, 0x2, 0xb3, 0xbb, 0xa)	46
6	0x165	(0x1, 0x1, 0xb3, 0x2c, 0x4, 0x9a)	46
7	0x165	(0x1, 0x2, 0x10, 0xb2, 0x58, 0xa4, 0x5c)	68
7	0x139	(0x1, 0x1, 0x21, 0x8, 0x96, 0x26, 0x98)	68
GF(2^4)			
3	0x1f	(0x2, 0xf, 0xc)	12
4	-		
5	0x13	(0x1, 0x2, 0x5, 0x4, 0x3)	14
6	-		

6 Conclusion

In this paper, we have presented a series of theory on generalized circulant matrices, so-called cyclic matrices, and also exploited the technique to successfully find the lightest MDS and involutory MDS matrices among this class of matrices with small orders. On one hand, cyclic matrices maintain the characteristics of circulant matrices, such as compact and flexible implementations in hardware and branch number in diffusion layer. On the other hand, they possess some advantages that circulant matrices cannot provide, for instance, the existence of involutory MDS matrices. The discovery of properties and constructions of MDS cyclic matrices may provide practical significance as well as theory value. Before this work, searching for the lightest MDS circulant matrices of order 8 are widely believed to be infeasible. Our results demonstrate an opposite view on this—we make it feasible under a credible metric—despite no guarantee of general case. As such, we can find the lightest MDS circulant matrices of order 8 which have less XOR count than the previously known ones in the literatures. Specially for the hash function WHIRLPOOL, we also provide a better MDS matrix which has smaller XOR count under the same setting. Although it is proven that IMDS left-circulant matrix of order 2^d does not exist, we find IMDS matrices for the other orders which forms a complement to the work in [21], where there exist only IMDS Hadamard matrices of order 2^d. All in all, we have found new lightweight MDS matrices that are flexible in hardware implementation and also a complete set of lightweight IMDS matrices for order $k \leq 8$.

Acknowledgements

The authors would like to thank Jian Guo, Gregor Leander, Thomas Peyrin, Yu Sasaki and the anonymous reviewers for their valuable suggestions.

References

1. E. Andreeva, B. Bilgin, A. Bogdanov, A. Luykx, F. Mendel, B. Mennink, N. Mouha, Q. Wang, and K. Yasuda. PRIMATEs v1. Submission to the CAESAR Competition, 2014. `http://competitions.cr.yp.to/round1/primatesv1.pdf`.
2. Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. Quark: A Lightweight Hash. In *CHES*, pages 1–15, 2010.
3. P. Barreto and V. Rijmen. The Anubis Block Cipher. Submission to the NESSIE Project, 2000.
4. P. Barreto and V. Rijmen. The Khazad Legacy-Level Block Cipher. First Open NESSIE Workshop, 2000.
5. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013.
6. A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, and I. Verbauwhede. SPONGENT: A Lightweight Hash Function. In *CHES*, pages 312–325, 2011.
7. 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 *CHES*, pages 450–466, 2007.

8. Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The Block Cipher Square. In *FSE*, pages 149–165, 1997.
9. Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.
10. Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON Family of Lightweight Hash Functions. In *CRYPTO*, pages 222–239, 2011.
11. Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED Block Cipher. In *CHES*, pages 326–341, 2011.
12. Kishan Chand Gupta and Indranil Ghosh Ray. On Constructions of Involutory MDS Matrices. In *Progress in Cryptology - AFRICACRYPT 2013, 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings*, pages 43–60, 2013.
13. Kishan Chand Gupta and Indranil Ghosh Ray. On Constructions of Circulant MDS Matrices for Lightweight Cryptography. In *ISPEC*, pages 564–576, 2014.
14. Kishan Chand Gupta and Indranil Ghosh Ray. Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. *Cryptography and Communications*, 7(2):257–287, 2015.
15. Jorge Nakahara Jr. and Élcio Abrahão. A New Involutory MDS Matrix for the AES. *I. J. Network Security*, 9(2):109–116, 2009.
16. Pascal Junod and Serge Vaudenay. Perfect diffusion primitives for block ciphers. In Helena Handschuh and M. Anwar Hasan, editors, *Selected Areas in Cryptography, 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers*, volume 3357 of *Lecture Notes in Computer Science*, pages 84–99. Springer, 2004.
17. Khoongming Khoo, Thomas Peyrin, Axel Y. Poschmann, and Huihui Yap. FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison. In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014*, volume 8731 of *Lecture Notes in Computer Science*, pages 433–450. Springer Berlin Heidelberg, 2014.
18. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1986.
19. D.J.S. Robinson. *An Introduction to Abstract Algebra*. De Gruyter textbook. Walter de Gruyter, 2003.
20. Claude E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, October 1949.
21. Siang Meng Sim, Khoongming Khoo, Frédérique Oggier, and Thomas Peyrin. Lightweight MDS Involution Matrices. In Gregor Leander, editor, *Fast Software Encryption*, volume 9054 of *Lecture Notes in Computer Science*, pages 471–493. Springer Berlin Heidelberg, 2015.
22. Serge Vaudenay. On the need for multipermutations: Cryptanalysis of MD4 and SAFER. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 286–297. Springer, 1994.
23. Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang Gong. The Simeck Family of Lightweight Block Ciphers. In Tim Güneysu and Helena Handschuh, editors, *Cryptographic Hardware and Embedded Systems - CHES 2015*, volume 9293 of *Lecture Notes in Computer Science*, pages 307–329. Springer, 2015.

A Generate Representatives for Equivalence Classes of Circulant Matrices

With the knowledge of equivalence classes of circulant matrices, what we need is an algorithm to pick one representative from each equivalence class and check if it is MDS. For simplicity, we focus on the index of the entries, the idea is to exhaust all non-$\mathcal{C}$-permutations. Before we describe how to generate the representatives, we introduce some notations and observations.

The position i, where $0 \leq i \leq k-1$, is the i-th entry of the first row of the circulant matrix of order k. For example, the first row of a circulant matrix of order 4 is given as (c_1, c_3, c_2, c_0), we can describe it as index 1 is in position 0, index 3 is in position 1, etc. The coprime positions consist of position i where i is coprime with k. In the earlier example, index 0 and 3 are in coprime positions.

Recall that σ is a $\mathcal{C}$-permutation if it is of the form $\sigma(i) = (bi + a) \bmod k$. We can always have a representative with index 0 at position 0 by applying a $\mathcal{C}$-permutation with $b = 1$ and $a \equiv -z \bmod k$, where index 0 is in position z. Therefore, without loss of generality, we fix index 0 at position 0 and hence $a = 0$.

One can observe that by apply some $\mathcal{C}$-permutation $\sigma(i) = bi \bmod k$, the indexes in coprime positions remain in coprime positions, similarly for the indexes in non-coprime positions. This is a direct result from the modulo arithmetic and we omit the proof as it can easily be verified. With this observation, we can choose any index which is in a coprime position x to be in position 1 by applying a $\mathcal{C}$-permutation with $b \equiv x^{-1} \bmod k$. Without loss of generality, we choose the smallest index among those in coprime positions to be in position 1 for the representatives.

With that, we can generate one representative for each equivalence classes by first fixing index 0 in position 0. Next, partition the remaining indexes into the coprime and non-coprime positions, choose the smallest index among those in coprime positions to be in position 1. Finally, permutate the remaining indexes within the coprime and non-coprime positions. The total number of representatives generated is

$$\binom{k-1}{\varphi(k)} \times (\varphi(k)-1)! \times (k-1-\varphi(k))! = \frac{(k-1)!}{\varphi(k)},$$

which is exactly the number of equivalence classes for a given order k from Theorem 1.

Example 5. For a circulant matrix of order 4, we let c_0 to be in position 0. We partition the remaining indexes into coprime and non-coprime positions, there are 3 ways to partition them. Finally, we pick the smallest index among those in coprime positions to be in position 1, we obtain $\{(1,1),(2,3) \mid (3,2)\}$, $\{(1,1),(3,3) \mid (2,2)\}$ and $\{(2,1),(3,3) \mid (1,2)\}$, where (x,y) means index x in position y. Thus we have a total of 3 representatives, namely (c_0, c_1, c_3, c_2), (c_0, c_1, c_2, c_3) and (c_0, c_2, c_1, c_3).

B Compact Equivalence Class of Hadamard Matrix

Definition 10. *A Hadamard matrix is a matrix of order 2^s, where $s > 0$, that can be defined by its first row of entries $\{h_0, h_1, ..., h_{2^s-1}\}$, and the (i,j)-entry can be expressed as $H[i,j] = h_{i \oplus j}$.*

In [21], the authors presented the equivalence classes of Hadamard matrices in terms of its branch number. First, let us recall the definition of the equivalence relation for the Hadamard matrices.

Definition 11. *[21] Let H and H^σ be two Hadamard matrices with the same multi-set of entries up to some permutation σ. We say that they are related, $H \sim H^\sigma$, if for every pair of input vectors, (u, u^σ), where u^σ is the vector u undergoing permutation σ, to H and H^σ respectively, have the same output vectors up to some permutation.*

More generally, the equivalence relation $\sim$ states that two matrices M and M' are related if there exists some permutation π such that for all input vectors u, Mu and $M'u'$ have the same output vectors up to some permutation, where u' is vector u that undergoes the permutation π.

Notice that the permutation σ from the above definition is equivalent to an index permutation in our context. In [21], the authors proved that if the index permutation σ is some $\mathcal{H}$-permutation, then $H \sim H^\sigma$. Its converse, however, remains an open question. More precisely, could there be other index permutations that also satisfy the equivalence relation $\sim$? Observing the similarity of this question and our work, we analyze the $\mathcal{H}$-permutation and the equivalence classes of Hadamard matrices and find that the answer is no. The $\mathcal{H}$-permutations have capture all possible index permutations that are related by $\sim$.

To prove this, we first show that our equivalence relation $\sim_\mathcal{B}$ and their equivalence relation $\sim$ are equivalent. Next, we show that "any index permutation σ that satisfies $H \sim_\mathcal{B} H^\sigma$ is a $\mathcal{H}$-permutation".

Proposition 7. *The equivalence relations $\sim$ and $\sim_\mathcal{B}$ are equivalent.*

Proof. ($\Rightarrow$) Suppose we have two matrices M and M' of order k such that $M \sim M'$. For any input vector u, the output vectors Mu and $M'u'$ are the same up to some permutation, where $u' = \pi(u)$. This permutation can be expressed as some right-multiplication permutation matrix P to the output vector. In addition, the permutation π on u can be expressed as some right-multiplication permutation matrix Q. Hence, we have $Mu = PM'Qu$. By considering $u = e_i, \forall i \in \{1, 2, ..., k\}$, where e_i is a vector of zeroes except the i-th position is 1. We can see that $M = PM'Q$, therefore $M \sim_\mathcal{B} M'$.

($\Leftarrow$) Given that $M = PM'Q$, for any vector u, we obtain $Mu = PM'u'$, where $u' = Qu$. This shows that there exists permutation Q such that the output vectors Mu and $M'u'$ are the same up to some permutation P. Hence, we have $M \sim M'$. □

Here, we give an equivalent but slightly different description for the $\mathcal{H}$-permutation, let σ be some $\mathcal{H}$-permutation, then σ satisfies

$$\sigma(i \oplus j) = \sigma(i) \oplus \sigma(j) \oplus \sigma(0),$$

where $i, j \neq 0$. The first two terms capture the condition that σ is linear if $\sigma(0) = 0$, and the term $\sigma(0)$ represents the permutation that picks row $\sigma(0)$ of a Hadamard matrix as the first row and generates a new Hadamard matrix under the same rule.

Theorem 5. *Given two Hadamard matrices H and H^σ, $H \sim_{\mathcal{B}} H^\sigma$ if and only if σ is some index permutation satisfying $\sigma(i \oplus j) = \sigma(i) \oplus \sigma(j) \oplus \sigma(0)$, $\forall i, j \in \{1, ..., 2^s - 1\}$.*

Proof. The "if" direction is proven in the original paper [21], hence we only need to prove the "only if" direction.

Given that $H \sim_{\mathcal{B}} H^\sigma$, by Definition 6, there exists permutation matrices P and Q such that $H^\sigma = PHQ$, where P (resp. Q) is in fact a row (resp. column) permutation on H. Suppose $\sigma(0) = a$, where $a \neq 0$, we can introduce an index permutation $\pi_a(i) = i \oplus a$ to obtain $(\pi_a \circ \sigma)(0) = 0$. Note that by the nature of the construction of Hadamard matrix, the index permutation π_a corresponds to a row permutation. Therefore, for any H^σ such that $H^\sigma = PHQ$, we can always apply some index permutation π_a to fix the first element h_0 and accordingly pre-multiply H^σ by a corresponding row permutation P_a, which gives $H^{\pi_a \circ \sigma} = P_a PHQ$, where $\pi_a(\sigma(0)) = 0$.

Next, we consider index permutation ϕ that fixes 0 and $H \sim_{\mathcal{B}} H^\phi$. For any submatrix M of H^ϕ formed by the same rows and columns $0, i, j, i \oplus j$, where $i \neq j$ and $i, j \in \{1, ..., 2^s - 1\}$. One can see that M consists of 4 coefficients, namely $h_0, h_{\phi(i)}, h_{\phi(j)}$ and $h_{\phi(i \oplus j)}$. Since $H^\phi = PHQ$, M of H^ϕ corresponds to some submatrix N of H.

Suppose row r_0 of H is one of the rows of N, then the 4 columns of H that make up N are columns $r_0, r_0 \oplus \phi(i), r_0 \oplus \phi(j)$ and $r_0 \oplus \phi(i \oplus j)$. Similarly, for another row r_1 of H that is also one of the rows of N, columns $r_1, r_1 \oplus \phi(i), r_1 \oplus \phi(j)$ and $r_1 \oplus \phi(i \oplus j)$ of H make up N. Since both sets of columns describe that same submatrix N of H, we want to find a matching between the two sets of columns $\{r_0, r_0 \oplus \phi(i), r_0 \oplus \phi(j), r_0 \oplus \phi(i \oplus j)\}$ and $\{r_1, r_1 \oplus \phi(i), r_1 \oplus \phi(j), r_1 \oplus \phi(i \oplus j)\}$, where $r_0 \neq r_1$. This implies $\{x, x \oplus \phi(i), x \oplus \phi(j), x \oplus \phi(i \oplus j)\} = \{0, \phi(i), \phi(j), \phi(i \oplus j)\}$ for some $x \neq 0$. Thus $x \in \{\phi(i), \phi(j), \phi(i \oplus j)\}$. If $x = \phi(i)$, then $\{x \oplus \phi(j), x \oplus \phi(i \oplus j)\} = \{\phi(j), \phi(i \oplus j)\}$ and thus $x \oplus \phi(j) = \phi(i \oplus j)$, that is, $\phi(i) \oplus \phi(j) = \phi(i \oplus j)$. Similarly, we can obtain $\phi(i \oplus j) = \phi(i) \oplus \phi(j)$ for the other cases. Therefore, if $H \sim_{\mathcal{B}} H^\phi$ with $\phi(0) = 0$, the index permutation ϕ satisfies the linear property $\phi(i \oplus j) = \phi(i) \oplus \phi(j)$.

Finally, we can see that if $H \sim_{\mathcal{B}} H^\sigma$ and we consider $\sigma = \pi_{\sigma(0)} \circ \phi$, then we have $\sigma(i \oplus j) = \sigma(i) \oplus \sigma(j) \oplus \sigma(0)$. □

This concludes that the equivalence classes of Hadamard matrices described in [21] is already the most compact classification of generic Hadamard matrix in terms of its branch number.