New Insights into Involutory and Orthogonal MDS Matrices

Yogesh Kumar[1], Susanta Samanta[2], and Atul Gaur[3]

[1] Scientific Analysis Group, DRDO, Metcalfe House Complex, Delhi-110054
adhana.yogesh@gmail.com

[2] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L3G1, Canada
ssamanta@uwaterloo.ca

[3] Department of Mathematics, University of Delhi, Delhi-110007
gaursatul@gmail.com

Abstract. MDS matrices play a critical role in the design of diffusion layers for block ciphers and hash functions due to their optimal branch number. Involutory and orthogonal MDS matrices offer additional benefits by allowing identical or nearly identical circuitry for both encryption and decryption, leading to equivalent implementation costs for both processes. These properties have been further generalized through the notions of semi-involutory and semi-orthogonal matrices. While much of the existing literature focuses on identifying efficiently implementable MDS candidates or proposing new constructions for MDS matrices of various orders, this work takes a different direction. Rather than introducing novel constructions or prioritizing implementation efficiency, we investigate structural relationships between the generalized variants and their conventional counterparts. Specifically, we establish nontrivial interconnections between semi-involutory and involutory matrices, as well as between semi-orthogonal and orthogonal matrices. Exploiting these relationships, we show that the number of semi-involutory MDS matrices can be directly derived from the number of involutory MDS matrices, and vice versa. A similar correspondence holds for semi-orthogonal and orthogonal MDS matrices. We also examine the intersection of these classes and show that the number of 3×3 MDS matrices that are both semi-involutory and semi-orthogonal coincides with the number of semi-involutory MDS matrices over $\mathbb{F}_{2^m}$. Furthermore, we derive the general structure of orthogonal matrices of arbitrary order n over $\mathbb{F}_{2^m}$. Based on this generic form, we provide a closed-form expression for enumerating all 3×3 orthogonal MDS matrices over $\mathbb{F}_{2^m}$. Finally, leveraging the aforementioned interconnections, we present explicit formulae for counting 3×3 semi-involutory MDS matrices and semi-orthogonal MDS matrices.

Keywords: Diffusion Layer · MDS matrix · Involutory matrix · Semi-involutory matrix · Orthogonal matrix · Semi-orthogonal matrix

1 Introduction

The concepts of confusion and diffusion [26] play a crucial role in the design of symmetric key cryptographic primitives. Confusion aims to create a complex statistical relationship between the ciphertext and the plaintext, making it difficult for an attacker to exploit. Typically, confusion is achieved through the interaction of non-linear S-boxes with mixing and shuffling processes over multiple rounds. Diffusion, on the other hand, ensures that a change in a single bit of the plaintext results in a significant change in approximately half of the bits in the ciphertext. Similarly, altering a single bit of the ciphertext should cause about half of the bits in the plaintext to change. This is related to the expectation that encryption schemes exhibit an avalanche effect [28]. In many block ciphers and hash functions, the diffusion property is achieved through the use of a linear layer, represented as a matrix. This matrix is designed to significantly alter the output in response to a small change in the input. Hence, MDS matrices find significant applications in the design of block ciphers and hash functions.

MDS matrices with specific properties, such as being involutory or orthogonal, are of particular importance. An involutory matrix is one that is its own inverse, while an orthogonal matrix has its transpose as its inverse. These characteristics facilitate implementation by enabling the use of identical or nearly identical circuitry for both encryption and decryption processes.

Researchers have consequently devoted considerable attention to involutory and orthogonal MDS matrices constructed from various canonical matrix families. Notably, Cauchy, Vandermonde, circulant, and Hadamard structures, as well as their generalizations, serve as rich sources for such matrices. The literature features many prominent examples, including those discussed in references [9–11, 17, 20, 22–24, 27, 30].

In addition to algebraic properties, several studies also focus on practical issues such as hardware cost and delay in the design and use of MDS matrices [6, 18, 19, 25, 29]. To further expand these foundational ideas, the concepts of semi-involutory [5] and semi-orthogonal [7] matrices have been introduced. The work in [2] represents the first systematic exploration of these generalized structures for the construction of semi-involutory and semi-orthogonal MDS matrices. Follow-up studies [3, 4, 16] have continued to advance this line of research.

Our Contribution. While much of the existing literature focuses on efficiently implementable MDS candidates or proposes new constructions for MDS matrices of various orders, this work adopts a different perspective by investigating structural relationships. In particular, we study the connections between generalized matrix forms, such as semi-involutory and semi-orthogonal matrices, and their conventional counterparts: involutory and orthogonal matrices. These relationships reveal deeper algebraic insights and provide a framework for systematically determining the number of MDS matrices that satisfy additional structural constraints.

More specifically, our key contributions are summarized as follows:

- We establish nontrivial connections between semi-involutory and involutory matrices, and between semi-orthogonal and orthogonal matrices over $\mathbb{F}_{2^m}$. These relationships enable bidirectional derivation: the number of semi-involutory MDS matrices over $\mathbb{F}_{2^m}$ determines the number of involutory MDS matrices over $\mathbb{F}_{2^m}$ and vice versa, with the same correspondence holding for semi-orthogonal and orthogonal MDS matrices.

- We characterize matrices that simultaneously satisfy both the semi-involutory and semi-orthogonal properties. Using this characterization, we prove that the number of 3×3 MDS matrices exhibiting both properties is equal to the number of 3×3 semi-involutory MDS matrices over $\mathbb{F}_{2^m}$.

- We derive the general structure of orthogonal matrices of arbitrary order n over $\mathbb{F}_{2^m}$. Specializing this result to the case $n = 3$, we prove that the number of 3×3 orthogonal MDS matrices over $\mathbb{F}_{2^m}$ is $(2^m - 2)(2^m - 3)(2^m - 4)$.

- We revisit the problem of enumerating 3×3 semi-involutory MDS matrices over $\mathbb{F}_{2^m}$. By leveraging the interconnection with involutory MDS matrices and applying known enumeration results from [12], we derive the enumeration formula for 3×3 semi-involutory MDS matrices over $\mathbb{F}_{2^m}$ through a more direct and concise approach. Similarly, we derive the number of 3×3 semi-orthogonal MDS matrices over $\mathbb{F}_{2^m}$.

- We extend our enumeration to 4×4 matrices by computing the number of semi-involutory MDS matrices over $\mathbb{F}_{2^m}$ for $m = 3, 4, \ldots, 8$, thereby extending the previously known results for $m = 3, 4$ [16] to larger finite field. Finally, Tables 4 and 5 present a comparison of the counts of 3×3 and 4×4 MDS matrices with various structural properties.

The structure of the paper is as follows. In Section 2, we provide a brief discussion of the mathematical background and notations employed throughout the paper. Section 3 establishes the interconnections between semi-involutory and involutory matrices, as well as between semi-orthogonal and orthogonal matrices. Section 4 analyzes the general structure of orthogonal matrices of arbitrary order n over $\mathbb{F}_{2^m}$ and presents a comparison of the counts of 3×3 and 4×4 MDS matrices with various structural properties. Finally, Section 5 concludes the paper.

2 Mathematical preliminaries

In this section, we discuss some definitions and mathematical preliminaries that are important in our context.

Let $\mathbb{F}_{2^m}$ be the finite field of order 2^m. We denote the multiplicative group of the finite field $\mathbb{F}_{2^m}$ by $\mathbb{F}_{2^m}^*$. The set of vectors of length n with entries from the finite field $\mathbb{F}_{2^m}$ is denoted by $\mathbb{F}_{2^m}^n$.

Let M be any $n \times n$ matrix over $\mathbb{F}_{2^m}$ and let $|M|$ denote its determinant. An $n \times n$ matrix is referred to as a matrix of order n. A matrix D of order n is diagonal if $(D)ij = 0$ for $i \neq j$. Using $d_i = (D)ii$, we represent the diagonal matrix D as $\mathrm{Diag}(d_1, d_2, \ldots, d_n)$. The determinant of D is $|D| = \prod_{i=1}^{n} d_i$. Hence, D is non-singular over $\mathbb{F}_{2^m}$ if and only if $d_i \neq 0$ for $1 \leq i \leq n$.

MDS matrix finds its practical applications as a diffusion layer in cryptographic primitives. The concept of the MDS matrix comes from coding theory, specifically from the realm of maximum distance separable (MDS) codes. An $[n, k, d]$ code is MDS if it meets the singleton bound $d = n - k + 1$.

Theorem 1. *[21, page 321] An $[n, k, d]$ code C with a generator matrix $G = [I \mid M]$, where M is a $k \times (n-k)$ matrix, is MDS if and only if every square submatrix (formed from any i rows and any i columns, for any $i = 1, 2, \ldots, min\{k, n-k\}$) of M is non-singular.*

Definition 1. *A matrix M of order n is said to be an MDS matrix if $[I \mid M]$ is a generator matrix of an $[2n, n]$ MDS code.*

Another way to define an MDS matrix is as follows:

Fact 1 *A square matrix M is an MDS matrix if and only if every square submatrix of M is non-singular.*

One of the elementary row operations on matrices is multiplying a row of a matrix by a non-zero scalar. MDS property remains invariant under such operations. Thus, we have the following result regarding MDS matrices.

Lemma 1. *[8] Let M be an MDS matrix, then for any non-singular diagonal matrices D_1 and D_2, $D_1 M D_2$ will also be an MDS matrix.*

Implementing involutory or orthogonal MDS matrices is more advantageous since it enables the use of an equivalent circuit or nearly equivalent circuit for both the encryption and decryption processes.

Definition 2. *An involutory matrix is defined as a square matrix M that is self-invertible or, equivalently, $M = M^{-1}$.*

Definition 3. *An orthogonal matrix is defined as a square matrix M whose inverse is its transpose or, equivalently, $M^{-1} = M^T$.*

In 2021, Cheon et al. [5] introduced the concept of semi-involutory property as a generalization of involutory property. The definition is provided below.

Definition 4. *[5] A non-singular matrix M is said to be semi-involutory if there exist two non-singular diagonal matrices D and D' such that $M^{-1} = DMD'$.*

We refer to the diagonal matrices D and D' as the corresponding diagonal matrices of the semi-involutory matrix M.
Furthermore, in 2012, Fiedler et al. [7] generalized orthogonal matrices and termed them G-matrices, which we refer to as semi-orthogonal matrices throughout this paper. The definition of a semi-orthogonal matrix is as follows:

Definition 5. *[7] A non-singular matrix M is semi-orthogonal if there exist two non-singular diagonal matrices D and D' such that $M^{-T} = DMD'$, where M^{-T} denotes the transpose of the matrix M^{-1}.*

Similar to semi-involutory matrices, we refer to the diagonal matrices D and D' as the corresponding diagonal matrices of the semi-orthogonal matrix M.

Lemma 2. *For any two non-singular diagonal matrices P and Q, if M is semi-involutory (or semi-orthogonal), then PMQ is also a semi-involutory (or semi-orthogonal) matrix.*

Proof. Let P and Q be two non-singular diagonal matrices. Suppose that M is a semi-involutory matrix with corresponding diagonal matrices D and D', i.e., $M^{-1} = DMD'$. Now, we have

$$\begin{aligned}(PMQ)^{-1} &= Q^{-1}M^{-1}P^{-1}\\ &= PP^{-1}Q^{-1}(DMD')P^{-1}QQ^{-1}\\ &= P^{-1}Q^{-1}D(PMQ)D'P^{-1}Q^{-1}.\end{aligned}$$

Since $P^{-1}Q^{-1}D$ and $D'P^{-1}Q^{-1}$ are also non-singular diagonal matrices, therefore, PMQ is a semi-involutory matrix. Similarly, we can prove that if M is a semi-orthogonal matrix, then PMQ is also a semi-orthogonal matrix. □

3 The Interconnections

In [15], the authors introduce a technique for generating all $n \times n$ MDS and involutory MDS matrices over $\mathbb{F}_{2^m}$. The proposed method involves first identifying $n \times n$ representative MDS matrices using a search-based approach. Subsequently, all $n \times n$ MDS and involutory MDS matrices can be obtained by multiplying two diagonal matrices with these representative matrices. To find all $n \times n$ representative MDS matrices, the authors define the representative matrix form M_1 over $\mathbb{F}^*_{2^m}$ as follows:

$$M_1 = \begin{pmatrix} 1 & 1 \dots 1 \\ 1 & \\ \vdots & R \\ 1 & \end{pmatrix}, \tag{1}$$

where R is a $(n-1) \times (n-1)$ matrix.

They also present the unique decomposition of a matrix M over $\mathbb{F}^*_{2^m}$ in the form $M = D_1 M_1 D_2$, where D_1 and D_2 are non-singular diagonal matrices. The result is stated below.

Theorem 2. *[15] Let $M = (m_{ij})$ be a $n \times n$ matrix over $\mathbb{F}_{2^m}^*$. Then, there exist unique $n \times n$ matrices D_1, D_2, and M_1 over $\mathbb{F}_{2^m}^*$ such that*

$$M = D_1 M_1 D_2,$$

where D_1 and D_2 are diagonal matrices, the first entry of D_2 is 1, and M_1 is a matrix of the form given in (1).

We will denote this unique decomposition as $M = \Phi(D_1, D_2, M_1)$. Throughout this section, all results are established over $\mathbb{F}_{2^m}^*$. Since MDS matrices inherently cannot contain zero entries, their properties align naturally with $\mathbb{F}_{2^m}^*$. To streamline the presentation, we will refer to the results as being over $\mathbb{F}_{2^m}$ when discussing MDS matrices throughout the paper.

3.1 The Interconnection between Involutory and Semi-involutory Matrices

In this section, we utilize the representative matrix form to derive the interconnections between semi-involutory and involutory matrices. Specifically, in Theorem 4, we establish that the number of $n \times n$ involutory MDS matrices over $\mathbb{F}_{2^m}$ is equal to $(2^m - 1)^{n-1}$ times the count of semi-involutory MDS matrices of order n of the form M_1 over $\mathbb{F}_{2^m}$. To derive Theorem 4, we first reference the theorem presented in [15].

Theorem 3. *[15] Let $M_1 = (c_{ij})$ be a matrix of order n over $\mathbb{F}_{2^m}^*$, as specified in (1), and $M_2 = (d_{ij})$ be its inverse. Then $\Phi(D_1, D_2, M_1)$ will be an involutory matrix if and only if $\exists\ \alpha_i \in \mathbb{F}_{2^m}^*$ such that*

$$d_{ij} = \alpha_i \alpha_j c_{ij},\ 1 \le i, j \le n.$$

Moreover, D_1 and D_2 must take the following form:

$$D_1 = \mathrm{Diag}(\alpha_1, \lambda_2, \lambda_3, \ldots, \lambda_n) \text{ and } D_2 = \mathrm{Diag}(1, \tfrac{\alpha_2}{\lambda_2}, \tfrac{\alpha_3}{\lambda_3}, \ldots, \tfrac{\alpha_n}{\lambda_n}),$$

where $\lambda_i \in \mathbb{F}_{2^m}^*$ for $i = 2, 3, \ldots, n$.

Corollary 1. *The number of involutory matrices of order n over $\mathbb{F}_{2^m}^*$ is given by*

$$(2^m - 1)^{n-1} \cdot N_1,$$

where N_1 denotes the number of semi-involutory matrices of order n over $\mathbb{F}_{2^m}^*$ of the form M_1, as specified in (1).

Proof. Let M be an involutory matrix of order n over $\mathbb{F}_{2^m}^*$. Then by Theorem 2, there exists a unique M_1 of the form of (1) such that $M = D_1 M_1 D_2$ for some non-singular diagonal matrices D_1 and D_2. Also, from Theorem 3, when M is involutory, D_1 and D_2 have the particular form. We can see that

$$M_1^{-1} = D_2 D_1 M_1 D_2 D_1.$$

Since D_2D_1 is again a non-singular diagonal matrix, from Definition 4, M_1 is a semi-involutory matrix with the corresponding diagonal matrices D and D', where $D = D' = D_2D_1$.

Moreover, it is possible to construct other involutory matrices by selecting different values for D_1 and D_2. However, according to Theorem 3, the matrix $\Phi(D_1, D_2, M_1)$ will be involutory only when D_1 and D_2 assume the specific form described. The scalar values λ_i for $i = 2, 3, \ldots, n$ can be chosen as any non-zero element from the field $\mathbb{F}_{2^m}$. Thus, in total, we have $(2^m - 1)^{n-1}$ possible choices for D_1 and D_2.

Hence, for a given semi-involutory matrix M_1, we can construct $(2^m - 1)^{n-1}$ distinct involutory matrices. Since each matrix M over $\mathbb{F}^*_{2^m}$ corresponds uniquely to an M_1, we conclude that the total number of involutory matrices over $\mathbb{F}^*_{2^m}$ is given by

$$(2^m - 1)^{n-1} \cdot N_1,$$

where N_1 represents the number of semi-involutory matrices of order n over $\mathbb{F}^*_{2^m}$ of the form M_1. $\square$

Thus, from the above corollary, we can easily derive the following result for involutory MDS matrices over the finite field $\mathbb{F}_{2^m}$.

Theorem 4. *The number of involutory MDS matrices of order n over $\mathbb{F}_{2^m}$ is given by*

$$(2^m - 1)^{n-1} \cdot N_2,$$

where N_2 denotes the number of semi-involutory MDS matrices of order n over $\mathbb{F}_{2^m}$ of the form M_1, as specified in (1).

Proof. Let $M = \Phi(D_1, D_2, M_1)$ be an involutory MDS matrix of order n over $\mathbb{F}_{2^m}$. Since D_1 and D_2 are non-singular matrices, by Lemma 1, M_1 is also an MDS matrix. Additionally, as M is an involutory matrix, Theorem 3 implies that M_1 is a semi-involutory matrix.

Now, since each MDS matrix M over $\mathbb{F}_{2^m}$ corresponds uniquely to an MDS matrix of the form M_1, we conclude from Corollary 1 [4] that the total number of involutory MDS matrices over $\mathbb{F}_{2^m}$ is given by

$$(2^m - 1)^{n-1} \cdot N_2,$$

where N_2 represents the number of semi-involutory MDS matrices of order n over $\mathbb{F}_{2^m}$ of the form M_1. $\square$

Now, we will discuss the results related to the semi-involutory MDS matrices over $\mathbb{F}_{2^m}$. For this purpose, we need the following lemma.

[4] It is worth noting that the result in Corollary 1 is stated for $\mathbb{F}^*_{2^m}$. However, since MDS matrices cannot contain zero entries, this condition is inherently satisfied by the results over $\mathbb{F}^*_{2^m}$. The same holds for the results in Theorems 5, 7, and 8, as they are derived from results over $\mathbb{F}^*_{2^m}$.

Lemma 3. *The number of semi-involutory matrices of order n over $\mathbb{F}_{2^m}^*$ is given by*

$$(2^m - 1)^{2n-1} \cdot N_1,$$

where N_1 denotes the number of semi-involutory matrices of order n over $\mathbb{F}_{2^m}^*$ of the form M_1, as specified in (1).

Proof. Let $M = \Phi(D_1, D_2, M_1)$ be a semi-involutory matrix over $\mathbb{F}_{2^m}^*$ with corresponding diagonal matrices D and D'. Thus, we have

$$\begin{aligned}
& M^{-1} = DMD' \\
\implies & M(DMD') = I \\
\implies & D_1 M_1 D_2 (D(D_1 M_1 D_2) D') = I \\
\implies & D_1 M_1 D_2 (D D_1 M_1 D_2 D') = I \\
\implies & M_1 (D_2 D D_1 M_1 D_2 D' D_1) = I.
\end{aligned}$$

Thus, the inverse of the matrix M_1 is given by

$$M_1^{-1} = D_2 D D_1 M_1 D_2 D' D_1.$$

Now, since $D_2 D D_1$ and $D_2 D' D_1$ are non-singular diagonal matrices, we can say that M_1 is also a semi-involutory matrix.
Conversely, suppose that M_1 is a semi-involutory matrix. Then, by Lemma 2, we can say that $M = \Phi(D_1, D_2, M_1) = D_1 M_1 D_2$ is also a semi-involutory matrix.

Therefore, we have established that $M = \Phi(D_1, D_2, M_1)$ is a semi-involutory matrix if and only if M_1 is a semi-involutory matrix.

Now, by selecting different values for D_1 and D_2, it is possible to construct other semi-involutory matrices from M_1. According to Theorem 2, we have $(2^m - 1)^{2n-1}$ possible choices for D_1 and D_2. Therefore, we conclude that the total number of semi-involutory matrices over $\mathbb{F}_{2^m}^*$ is given by

$$(2^m - 1)^{2n-1} \cdot N_1,$$

where N_1 represents the number of semi-involutory matrices of order n over $\mathbb{F}_{2^m}^*$ of the form M_1. □

Similar to Theorem 4, using the above lemma, we can easily derive the result for semi-involutory MDS matrices over $\mathbb{F}_{2^m}$. Thus, we provide the result without proof.

Theorem 5. *The number of semi-involutory MDS matrices of order n over $\mathbb{F}_{2^m}$ is given by*

$$(2^m - 1)^{2n-1} \cdot N_2,$$

where N_2 denotes the number of semi-involutory MDS matrices of order n over $\mathbb{F}_{2^m}$ of the form M_1, as specified in (1).

In the following lemma, we mention the explicit formula obtained in [12] for enumerating all 3×3 involutory MDS matrices over $\mathbb{F}_{2^m}$.

Lemma 4. *[12] For $m \geq 3$, the number of all 3×3 involutory MDS matrices over $\mathbb{F}_{2^m}$ is given by $(2^m - 1)^2(2^m - 2)(2^m - 4)$.*

Corollary 2. *For $m \geq 3$, the number of semi-involutory MDS matrices of order 3 over $\mathbb{F}_{2^m}$ is $(2^m - 1)^5(2^m - 2)(2^m - 4)$.*

Proof. From the above lemma, we know that the number of all 3×3 involutory MDS matrices is $(2^m - 1)^2(2^m - 2)(2^m - 4)$. Therefore, from Theorem 4, we have

$$\begin{aligned}
&(2^m - 1)^2(2^m - 2)(2^m - 4) = (2^m - 1)^2 \cdot N_2 \\
\implies &N_2 = (2^m - 2)(2^m - 4).
\end{aligned}$$

Here N_2 denotes the number of semi-involutory MDS matrices of order 3 over $\mathbb{F}_{2^m}$ of the form M_1, as specified in (1).

Therefore, from Theorem 5, the count of semi-involutory MDS matrices of order 3 over $\mathbb{F}_{2^m}$ is given by

$$\begin{aligned}
&(2^m - 1)^{2\cdot 3-1} \cdot N_2 \\
=&(2^m - 1)^5(2^m - 2)(2^m - 4).
\end{aligned}$$

□

Remark 1. We note that the enumeration formula for 3×3 semi-involutory MDS matrices over $\mathbb{F}_{2^m}$ has been previously established by Chatterjee et al. [3] through a comprehensive proof, and independently derived in recent work by Kumar et al. [16]. Our approach complements these results by leveraging the structural interconnection with involutory MDS matrices, which yields an alternative derivation that is more direct and concise.

In [14], the authors propose a matrix form for generating all 4×4 involutory MDS matrices over the field $\mathbb{F}_{2^m}$. Their approach specifically involves searching for these representative matrices within a set of cardinality $(2^m - 1)^5$, facilitating the explicit enumeration of the total number of 4×4 involutory MDS matrices over $\mathbb{F}_{2^m}$ for $m = 3, 4, \ldots, 8$. We take their results and combine Theorems 4 and 5 to derive the exact count of 4×4 semi-involutory MDS matrices over $\mathbb{F}_{2^m}$. For example, as derived in [14], the count of 4×4 involutory MDS matrices over $\mathbb{F}_{2^3}$ is $7^3 \times 48$. By applying Theorem 4, the number of semi-involutory MDS matrices of the form M_1 is 48. Therefore, using Theorem 5, we conclude that the number of 4×4 semi-involutory MDS matrices over $\mathbb{F}_{2^3}$ is $7^7 \times 48$. Similarly, we can derive the count for the finite fields $\mathbb{F}_{2^m}$, where $m = 4, \ldots, 8$. A comparison of the counts for 4×4 involutory and semi-involutory MDS matrices is presented in Table 1.

3.2 The Interconnection between Orthogonal and Semi-orthogonal Matrices

In this section, we utilize the representative matrix form M_1, as defined in (1), to explore the interconnections between semi-orthogonal and orthogonal matrices.

Table 1. Count of 4×4 involutory and semi-involutory MDS Matrices

Finite Field	Semi-involutory M_1	Involutory	Semi-involutory
$\mathbb{F}_{2^3}$	48	$7^3 \times 48$	$7^7 \times 48$
$\mathbb{F}_{2^4}$	71856	$15^3 \times 71856$	$15^7 \times 71856$
$\mathbb{F}_{2^5}$	10188240	$31^3 \times 10188240$	$31^7 \times 10188240$
$\mathbb{F}_{2^6}$	612203760	$63^3 \times 612203760$	$63^7 \times 612203760$
$\mathbb{F}_{2^7}$	26149708368	$127^3 \times 26149708368$	$127^7 \times 26149708368$
$\mathbb{F}_{2^8}$	961006331376	$255^3 \times 961006331376$	$255^7 \times 961006331376$

Specifically, in Theorem 8, we demonstrate that the number of orthogonal MDS matrices of order n over $\mathbb{F}_{2^m}$ corresponds to the count of semi-orthogonal MDS matrices of order n of the form M_1. To establish this relationship, we present the following theorem.

Theorem 6. *Let $M_1 = (c_{ij})$ be a matrix of order n over $\mathbb{F}_{2^m}^*$ of the form given in (1) and $M_2 = (d_{ij})$ be its inverse. Then $M = \Phi(D_1, D_2, M_1)$ is an orthogonal matrix if and only if M_1 is a semi-orthogonal matrix such that*

$$M_1^{-T} = D_1^2 M_1 D_2^2.$$

Moreover, D_1 and D_2 must take the following form:

$$D_1 = \mathrm{Diag}(\sqrt{d_{11}}, \sqrt{d_{12}}, \ldots, \sqrt{d_{1n}}) \text{ and } D_2 = \mathrm{Diag}(1, \sqrt{\tfrac{d_{21}}{d_{11}}}, \ldots, \sqrt{\tfrac{d_{n1}}{d_{11}}}).$$

Proof. Let $D_1 = \mathrm{Diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and $D_2 = \mathrm{Diag}(1, \theta_2, \ldots, \theta_n)$ be two non-singular diagonal matrices over $\mathbb{F}_{2^m}$. Suppose that $M = \Phi(D_1, D_2, M_1)$ is an orthogonal matrix. Thus, we have

$$\begin{aligned}
& MM^T = I \\
\implies\ & (D_1 M_1 D_2)(D_2 M_1^T D_1) = I \\
\implies\ & D_1 M_1 D_2^2 M_1^T = D_1^{-1} \\
\implies\ & D_1^2 M_1 D_2^2 M_1^T = I \\
\implies\ & M_1^{-T} = D_1^2 M_1 D_2^2.
\end{aligned}$$

Since D_1^2 and D_2^2 are non-singular diagonal matrices, we can conclude that M_1 is a semi-orthogonal matrix. Moreover, since $M_2 = (d_{ij})$ is the inverse of M_1, we also have the relation

$$d_{ji} = \lambda_i^2 c_{ij} \theta_j^2.$$

If we compare the first row and first column entries, since $c_{i1} = c_{1j} = 1$ for $1 \leq i, j \leq n$, we have

$$d_{i1} = \lambda_1^2 \theta_i^2 \ \text{ and } \ d_{1j} = \theta_1^2 \lambda_j^2 \ \text{ for } \ 1 \leq i, j \leq n.$$

Since $\theta_1 = 1$, it follows that $d_{11} = \lambda_1^2$, which implies that $d_{11} \neq 0$. Furthermore, we have the following relations

$$\lambda_i = \sqrt{d_{1i}} \quad \text{and} \quad \theta_i = \sqrt{\frac{d_{i1}}{d_{11}}} \quad \text{for} \quad 1 \leq i \leq n.$$

It is important to note that we are working in a finite field of characteristic 2, which ensures the existence of square roots in the above equations. Consequently, the diagonal matrices D_1 and D_2 assume the desired form as stated in the theorem.

Conversely, suppose that M_1 is a semi-orthogonal matrix such that

$$M_1^{-T} = D_1^2 M_1 D_2^2,$$

where D_1 and D_2 has the following form

$$D_1 = \text{Diag}(\sqrt{d_{11}}, \sqrt{d_{12}}, \ldots, \sqrt{d_{1n}}) \text{ and } D_2 = \text{Diag}(1, \sqrt{\tfrac{d_{21}}{d_{11}}}, \ldots, \sqrt{\tfrac{d_{n1}}{d_{11}}}).$$

Thus, we obtain the following expression

$$d_{ji} = \lambda_i^2 c_{ij} \theta_j^2 \quad \text{for} \quad 1 \leq i, j \leq n. \tag{2}$$

Now, we will show that $M = \Phi(D_1, D_2, M_1)$ is an orthogonal matrix. If $M = (m_{ij})$ then we have $m_{ij} = \lambda_i \theta_j c_{ij}$ for $1 \leq i, j \leq n$. Therefore, we have

$$\begin{aligned}
(MM^T)_{ij} &= \sum_{k=1}^{n} m_{ik} m_{jk} \\
&= \sum_{k=1}^{n} (\lambda_i \theta_k c_{ik})(\lambda_j \theta_k c_{jk}) \\
&= \sum_{k=1}^{n} \lambda_i \lambda_j c_{ik} \theta_k^2 c_{jk} \\
&= \sum_{k=1}^{n} \lambda_i \lambda_j c_{ik} \frac{d_{kj}}{\lambda_j^2} \quad \text{[From Equation 2]} \\
&= \frac{\lambda_i}{\lambda_j} \sum_{k=1}^{n} c_{ik} d_{kj} \\
&= \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases} \quad [\text{Since } M_2 = M_1^{-1}]
\end{aligned}$$

This demonstrates that $MM^T = I$, implying that M is an orthogonal matrix. This completes the proof. □

Corollary 3. *The number of orthogonal matrices of order n over $\mathbb{F}_{2^m}^*$ is equal to the number of semi-orthogonal matrices of order n over $\mathbb{F}_{2^m}^*$ of the form M_1, as specified in (1).*

Proof. Let M be an orthogonal matrix of order n over $\mathbb{F}_{2^m}^*$. By Theorem 2, there exists a unique matrix M_1 in the form of (1) such that $M = D_1 M_1 D_2$, where D_1 and D_2 are non-singular diagonal matrices.

According to Theorem 6, M_1 is a semi-orthogonal matrix, with D_1^2 and D_2^2 as the corresponding diagonal matrices. Furthermore, D_1 and D_2 assume the specific forms described in Theorem 6, which ensures that the choice of D_1 and D_2 is unique when M is orthogonal.

Thus, for a given semi-orthogonal matrix M_1, there is a unique construction of an orthogonal matrix M. Consequently, the total number of orthogonal matrices over $\mathbb{F}_{2^m}^*$ is equal to the number of semi-orthogonal matrices of order n over $\mathbb{F}_{2^m}^*$ of the form M_1. □

If $M = \Phi(D_1, D_2, M_1)$ is an MDS matrix of order n over $\mathbb{F}_{2^m}$, then by Lemma 1, M_1 is also an MDS matrix. Furthermore, if M is an orthogonal MDS matrix, Theorem 6 implies that M_1 is a semi-orthogonal MDS matrix. Therefore, based on Corollary 3, we can conclude the following result.

Theorem 7. *The number of orthogonal MDS matrices of order n over $\mathbb{F}_{2^m}$ is equal to the number of semi-orthogonal MDS matrices of order n over $\mathbb{F}_{2^m}$ of the form M_1, as specified in (1).*

We now turn our attention to the results concerning semi-orthogonal MDS matrices over $\mathbb{F}_{2^m}$. To facilitate this discussion, we present the following lemma. The proof of this lemma closely resembles that of Lemma 3. Nevertheless, for the sake of completeness, we provide it here.

Lemma 5. *The number of semi-orthogonal matrices of order n over $\mathbb{F}_{2^m}^*$ is given by*

$$(2^m - 1)^{2n-1} \cdot N_3,$$

where N_3 denotes the number of semi-orthogonal matrices of order n over $\mathbb{F}_{2^m}^*$ of the form M_1, as specified in (1).

Proof. Let $M = \Phi(D_1, D_2, M_1)$ be a semi-orthogonal matrix over $\mathbb{F}_{2^m}^*$ with corresponding diagonal matrices D and D' . Thus, we have

$$\begin{aligned} & M^{-T} = DMD' \\ \implies & M^T(DMD') = I \\ \implies & D_2 M_1^T D_1 D(D_1 M_1 D_2) D' = I \\ \implies & M_1^T(DD_1^2 M_1 D_2^2 D') = I. \end{aligned}$$

Thus, the inverse of the matrix M_1 is given by

$$M_1^{-T} = DD_1^2 M_1 D_2^2 D'.$$

Now, since DD_1^2 and $D_2^2 D'$ are non-singular diagonal matrices, we can say that M_1 is also a semi-orthogonal matrix.

Conversely, suppose that M_1 is a semi-orthogonal matrix. Then, by Lemma 2, we can say that $M = \Phi(D_1, D_2, M_1) = D_1 M_1 D_2$ is also a semi-orthogonal matrix.

Therefore, we have established that $M = \Phi(D_1, D_2, M_1)$ is a semi-orthogonal matrix if and only if M_1 is a semi-orthogonal matrix.

Now, by selecting different values for D_1 and D_2, it is possible to construct other semi-orthogonal matrices from M_1. According to Theorem 2, we have $(2^m - 1)^{2n-1}$ possible choices for D_1 and D_2. Therefore, we conclude that the total number of semi-orthogonal matrices over $\mathbb{F}_{2^m}^*$ is given by

$$(2^m - 1)^{2n-1} \cdot N_3,$$

where N_3 represents the number of semi-orthogonal matrices of order n over $\mathbb{F}_{2^m}^*$ of the form M_1. $\square$

Similar to Theorem 5, using the above lemma, we can easily derive the result for semi-orthogonal MDS matrices over $\mathbb{F}_{2^m}$. Thus, we provide the result without proof.

Theorem 8. *The number of semi-orthogonal MDS matrices of order n over $\mathbb{F}_{2^m}$ is given by*

$$(2^m - 1)^{2n-1} \cdot N_4,$$

where N_4 denotes the number of semi-orthogonal MDS matrices of order n over $\mathbb{F}_{2^m}$ of the form M_1, as specified in (1).

In the existing literature, a precise count of the 3×3 orthogonal MDS matrices over $\mathbb{F}_{2^m}$ has not been established. In Theorem 13, we derive an explicit formula for the enumeration of 3×3 orthogonal MDS matrices over $\mathbb{F}_{2^m}$. Furthermore, by utilizing Theorems 7 and 8, we obtain an explicit formula for counting the 3×3 semi-orthogonal MDS matrices over $\mathbb{F}_{2^m}$.

In Theorem 12, we establish a matrix structure for the $n \times n$ orthogonal matrices. Utilizing this structure, we are able to determine the count of 4×4 orthogonal MDS matrices over $\mathbb{F}_{2^m}$ for $m = 3$ and 4. Subsequently, by applying Theorems 7 and 8, we derive the count of 4×4 semi-orthogonal MDS matrices over $\mathbb{F}_{2^m}$ for the same values of m. The results are presented in Table 2.

Table 2. Count of 4×4 orthogonal and semi-orthogonal MDS Matrices

Finite Field	Semi-orthogonal of the form M_1	Orthogonal	Semi-orthogonal
$\mathbb{F}_{2^3}$	720	720	$7^7 \times 720$
$\mathbb{F}_{2^4}$	1147440	1147440	$15^7 \times 1147440$

3.3 The Interconnection between Semi-Involutory and Semi-Orthogonal Matrices

In this section, we will discuss the case when a matrix possesses both the properties of being semi-involutory and semi-orthogonal. It is straightforward to observe that if a matrix M is symmetric, then M is semi-involutory if and only if it is semi-orthogonal. However, the question arises whether this relationship holds for matrices that are not necessarily symmetric. The following theorem aims to generalize this condition for matrices that exhibit both semi-orthogonal and semi-involutory properties.

Theorem 9. *[5] Let M be a non-singular matrix of order n. Suppose $M = DM^TD'$ for some non-singular diagonal matrices D and D'. Then M is semi-involutory if and only if M is a semi-orthogonal matrix.*

In Lemma 3, we establish that the matrix $M = \Phi(D_1, D_2, M_1)$ is a semi-involutory matrix if and only if M_1 is semi-involutory. Similarly, in Lemma 5, we demonstrate that $M = \Phi(D_1, D_2, M_1)$ is a semi-orthogonal matrix if and only if M_1 is semi-orthogonal. Therefore, to determine whether the matrix M is both semi-involutory and semi-orthogonal, we must examine the case in which M_1 possesses both properties. The following theorem addresses this result.

Theorem 10. *Let $M_1 = (c_{ij})$ be a matrix of order n of the form given in (1) and suppose that $M_1 = DM_1^TD'$ for some non-singular diagonal matrices D and D'. Then M_1 is a symmetric matrix.*

Proof. Suppose that $M_1 = DM_1^TD'$ for some non-singular diagonal matrices D and D', where $D = \text{Diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $D' = \text{Diag}(\beta_1, \beta_2, \ldots, \beta_n)$. Thus, we have

$$c_{ij} = \alpha_i c_{ji} \beta_j \quad \text{for } 1 \leq i, j \leq n. \tag{3}$$

If we compare the first row, first column, and diagonal entries, since $c_{i1} = c_{1j} = 1$ for $1 \leq i, j \leq n$, we have

$$\begin{aligned} \alpha_1\beta_j &= 1 \text{ for } 1 \leq j \leq n \\ \alpha_i\beta_1 &= 1 \text{ for } 1 \leq i \leq n \\ \alpha_i\beta_i &= 1 \text{ for } 1 \leq i \leq n. \end{aligned}$$

After solving this system of equations, we have

$$\alpha_1 = \alpha_2 = \ldots \alpha_n, \text{ and } \beta_1 = \beta_2 = \ldots \beta_n.$$

By putting these values of α_i's and β_i's for $1 \leq i \leq n$ in (3) we get

$$c_{ij} = c_{ji} \quad \text{for } 1 \leq i, j \leq n.$$

Therefore, we have $M_1 = M_1^T$. This completes the proof. □

The next Lemma shows that the semi-involutory matrix of order 3 over $\mathbb{F}_{2^m}^*$ of the form M_1 is symmetric.

Lemma 6. *Let M_1 be a semi-involutory matrix of order 3 over $\mathbb{F}_{2^m}^*$. Then M_1 is a symmetric matrix.*

Proof. Let

$$M_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & a & b \\ 1 & c & d \end{pmatrix}$$

be a semi-involutory matrix and $D = \mathrm{Diag}(\alpha_1, \alpha_2, \alpha_3)$ and $D' = \mathrm{Diag}(\beta_1, \beta_2, \beta_3)$ be the corresponding diagonal matrices. Thus, we have

$$\begin{aligned} & DM_1D' = M_1^{-1} \\ \implies & DM_1D'M_1 = I. \end{aligned}$$

Since $(DM_1D'M_1)_{12} = (DM_1D'M_1)_{21} = 0$, we have

$$\beta_1 = a\beta_2 + c\beta_3 \quad \text{and } \beta_1 = a\beta_2 + b\beta_3.$$

Adding these two equations, we can derive that $b = c$.

Therefore, M_1 is a symmetric matrix. This completes the proof. ☐

Remark 2. From Lemma 6, we know that any 3×3 semi-involutory of the form M_1 is always symmetric. Additionally, by applying Theorems 9 and 10, we can conclude that the number of 3×3 matrices, of the form M_1, that are both semi-involutory and semi-orthogonal is equal to the number of 3×3 semi-involutory matrices of the form M_1 over $\mathbb{F}_{2^m}^*$.

Theorem 11. *For $m \geq 3$, the count of all 3×3 MDS matrices possessing both semi-involutory and semi-orthogonal properties over $\mathbb{F}_{2^m}$ is $(2^m - 1)^5(2^m - 2)(2^m - 4)$.*

Remark 3. It is worth mentioning that Lemma 6 is not true for higher orders. For example, consider the matrix

$$M_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha^{10} & \alpha^2 \\ 1 & \alpha^8 & \alpha^5 & \alpha^{11} \end{pmatrix}$$

over $\mathbb{F}_{2^4}^*$, where α is a primitive element and a root of the constructing polynomial $x^4 + x + 1$. It can be checked that the matrix M_1 is semi-involutory with the corresponding diagonal matrices $D = (1, \alpha^{12}, \alpha, \alpha^{11})$ and $D' = (\alpha^{14}, \alpha^{11}, 1, \alpha^{10})$. However, the matrix M_1 is not symmetric. This implies that over $\mathbb{F}_{2^m}^*$, the count of higher order (say ≥ 4) matrices that are both semi-involutory and semi-orthogonal may not be the same as the number of semi-involutory matrices of that order.

In Table 3, we present the count of MDS matrices of order 4 that possess both semi-involutory and semi-orthogonal properties.

Table 3. Count of 4×4 MDS matrices with both semi-involutory and semi-orthogonal properties

Finite Field	The matrix M_1 with both properties	Total Count
$\mathbb{F}_{2^3}$	48	$7^7 \times 48$
$\mathbb{F}_{2^4}$	11088	$15^7 \times 11088$

Remark 4. From Tables 1 and 3, we can observe that the number of 4×4 MDS matrices that are both semi-involutory and semi-orthogonal is equal to the number of 4×4 semi-involutory MDS matrices over $\mathbb{F}_{2^3}$. This equivalence arises because there are no non-symmetric semi-involutory MDS matrices of order 4 over $\mathbb{F}_{2^3}$ of the form M_1. In contrast, among the semi-involutory MDS matrices of the form M_1 of order 4 over $\mathbb{F}_{2^4}$, we find 60768 non-symmetric matrices and 11088 symmetric matrices. This discrepancy leads to a different count for the matrices over the field $\mathbb{F}_{2^4}$.

4 On the Structure of Orthogonal MDS Matrices

In this section, we begin by examining the structure of orthogonal matrices of order n over $\mathbb{F}_{2^m}$. We then establish that the number of orthogonal MDS matrices of order 3 over $\mathbb{F}_{2^m}$ is given by $(2^m-2)(2^m-3)(2^m-4)$. Additionally, we provide the explicit count of orthogonal MDS matrices of order 4 over $\mathbb{F}_{2^m}$ for $m=3$ and $m=4$. In the following theorem, we derive the general form of orthogonal matrices of order n over $\mathbb{F}_{2^m}$.

Theorem 12. *Let $M=(m_{ij})$ be a $n \times n$ matrix over $\mathbb{F}_{2^m}$. Then M is orthogonal if and only if M can be expressed in the following form:*

$$\begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n-1} & b_1+1 \\ m_{21} & m_{22} & \dots & m_{2n-1} & b_2+1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ m_{n-11} & m_{n-12} & \dots & m_{n-1n-1} & b_{n-1}+1 \\ c_1+1 & c_2+1 & \dots & c_{n-1}+1 & \sum_{i=1}^{n-1}(b_i+1)+1 \end{pmatrix},$$

where $b_i=\sum_{j=1}^{n-1} m_{ij}$, $c_j=\sum_{i=1}^{n-1} m_{ij}$, $1 \leq i,j \leq n-1$ and m_{ij}'s satisfy the following equations for $1 \leq k < l \leq n-1$

$$\sum_{i=1}^{n-1} \sum_{j=1, j\neq i}^{n-1} m_{ki}m_{lj} + b_k + b_l = 1 \tag{4}$$

$$\sum_{i=1}^{n-1} \sum_{j=1, j\neq i}^{n-1} m_{ik}m_{jl} + c_k + c_l = 1. \tag{5}$$

Proof. Let

$$M = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ m_{21} & m_{22} & \dots & m_{2n} \\ m_{31} & m_{32} & \dots & m_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{pmatrix}$$

be a $n \times n$ orthogonal matrix over $\mathbb{F}_{2^m}$. Since M is orthogonal, then $MM^T = M^T M = I$, where I is a $n \times n$ identity matrix. Let R_i and C_i be the ith row and column vectors of M. We have

$$R_i \cdot R_j = C_i \cdot C_j = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases} \tag{6}$$

For $i = j$, we get the following values of m_{in} and m_{nj}, $1 \leq i, j \leq n$.

$$\left.\begin{aligned} m_{1n} &= \textstyle\sum_{j=1}^{n-1} m_{1j} + 1 = b_1 + 1 \\ &\vdots \\ m_{n-1n} &= \textstyle\sum_{j=1}^{n-1} m_{n-1j} + 1 = b_{n-1} + 1 \\ m_{n1} &= \textstyle\sum_{i=1}^{n-1} m_{i1} + 1 = c_1 + 1 \\ &\vdots \\ m_{nn-1} &= \textstyle\sum_{i=1}^{n-1} m_{in-1} + 1 = c_{n-1} + 1 \\ m_{nn} &= \textstyle\sum_{i=1}^{n-1} (b_i + 1) + 1 = \sum_{j=1}^{n-1} (c_j + 1) + 1 \end{aligned}\right\} \tag{7}$$

where $b_i = \sum_{j=1}^{n-1} m_{ij}$ and $c_j = \sum_{i=1}^{n-1} m_{ij}$, $1 \leq i, j \leq n-1$.

From (6), let's consider the dot product of any two distinct rows (columns) of the first $(n-1)$ rows (columns) of M which is zero. Thus, for $1 \leq k < l \leq n-1$, we have the following equations

$$R_k \cdot R_l = 0 \tag{8}$$

$$C_k \cdot C_l = 0. \tag{9}$$

The equations $R_i \cdot R_n = 0$ and $C_i \cdot C_n = 0$ for $1 \leq i \leq n-1$ are redundant because they can be derived from the set of equations (7), (8) and (7), (9), respectively.

Now, by substituting the values of m_{kn} and m_{ln} in (8), we get the following relation

$$\sum_{i=1}^{n-1}\sum_{j=1,j\neq i}^{n-1} m_{ki}m_{lj}+\sum_{i=1}^{n-1}(m_{ki}+m_{li})=\sum_{i=1}^{n-1}\sum_{j=1,j\neq i}^{n-1} m_{ki}m_{lj}+b_k+b_l=1.$$

Similarly, by substituting the values of m_{nk} and m_{nl} in (9), we get the following relation

$$\sum_{i=1}^{n-1}\sum_{j=1,j\neq i}^{n-1} m_{ik}m_{jl}+\sum_{i=1}^{n-1}(m_{ik}+m_{il})=\sum_{i=1}^{n-1}\sum_{j=1,j\neq i}^{n-1} m_{ik}m_{jl}+c_k+c_l=1.$$

Thus, we obtain the desired form for M. This completes the proof. □

There have been numerous studies on $2^n \times 2^n$ MDS matrices that focus on efficient implementation. However, other dimensions have not been explored as thoroughly. Since sub-matrices of an MDS matrix are also MDS, studying the structure of 3×3 MDS matrices could be useful in generating higher order MDS matrices. In addition, 3×3 MDS matrices that are involutory or orthogonal can be valuable in the design of lightweight block ciphers and hash functions with non-standard block or key sizes. For example, in [1], the CURUPIRA block cipher, designed for constrained platforms, was introduced. CURUPIRA operates on 96-bit plaintext blocks with key sizes of 96, 144, or 192 bits. The diffusion layer of CURUPIRA employs a 3×3 MDS matrix over $\mathbb{F}_{2^8}$. In Theorem 13, we provide an explicit formula for counting 3×3 orthogonal MDS matrices over $\mathbb{F}_{2^m}$. To derive this formula, we first identify the generic form of 3×3 orthogonal matrices in Corollary 4, which is established using Theorem 12. Additionally, by analyzing Equations 4 and 5, we find that they reduce to a single equation

$$m_{11}m_{22}+m_{12}m_{21}+m_{11}+m_{12}+m_{21}+m_{22}=1$$

for a 3×3 orthogonal matrix over $\mathbb{F}_{2^m}$. This leads to the following characterization of such matrices.

Corollary 4. *Let $M=(m_{ij})$ be a 3×3 matrix over $\mathbb{F}_{2^m}$. Then M is orthogonal if and only if M can be expressed in the following form*

$$\begin{pmatrix} m_{11} & m_{12} & m_{11}+m_{12}+1 \\ m_{21} & m_{22} & m_{21}+m_{22}+1 \\ m_{11}+m_{21}+1 & m_{12}+m_{22}+1 & m_{11}+m_{12}+m_{21}+m_{22}+1 \end{pmatrix},$$

where $m_{11}m_{22}+m_{12}m_{21}+m_{11}+m_{12}+m_{21}+m_{22}=1$.

The explicit formula for counting orthogonal MDS matrices of order 3 over $\mathbb{F}_{2^m}$ is obtained in the following theorem.

Theorem 13. *For $m \geq 3$, the number of all orthogonal MDS matrices of order 3 over $\mathbb{F}_{2^m}$ is $(2^m-2)(2^m-3)(2^m-4)$.*

Proof. Let M be a 3×3 matrix of the form as defined in Corollary 4. From the definition of an MDS matrix, every square sub-matrix of an MDS matrix is non-singular. Since the inverse of an orthogonal matrix is the transpose of that matrix, if all the elements of an orthogonal matrix are non-zero, then all the minors of order 1 and 2 of that matrix are non-zero. Therefore, M is MDS if and only if all elements of M are non-zero, i.e.,

$$\begin{aligned} & m_{11}, m_{12}, m_{21}, m_{22} \in \mathbb{F}_{2^m}^*, m_{12} \neq m_{11}+1, m_{21} \neq m_{11}+1 \\ & m_{22} \neq m_{12}+1, m_{22} \neq m_{21}+1, m_{22} \neq m_{11}+m_{12}+m_{21}+1. \end{aligned} \tag{10}$$

We will now analyze two cases to determine the count of all orthogonal MDS matrices of order 3.

Case I: $m_{11} = 1$. From (10), we have the following conditions on the parameters of M

$$\begin{aligned} & m_{12}, m_{21}, m_{22} \in \mathbb{F}_{2^m}^*, m_{22} \neq m_{12}+1, m_{22} \neq m_{21}+1 \\ & m_{22} \neq m_{12}+m_{21}. \end{aligned}$$

The parameters of M also satisfy the following relation

$$m_{11}m_{22} + m_{12}m_{21} + m_{11} + m_{12} + m_{21} + m_{22} = 1.$$

Since $m_{11} = 1$, it follows that $m_{12}m_{21} = m_{12} + m_{21}$. Now, suppose $m_{12} = 1$. Substituting this into the equation, we get $m_{21} = 1 + m_{21}$, which leads to a contradiction. Therefore, $m_{12} \neq 1$. Consequently, $m_{21} = (m_{12}+1)^{-1}m_{12}$.

In this case, the number of all orthogonal MDS matrices of order 3 over $\mathbb{F}_{2^m}$ is equal to the cardinality of the set S_1, defined as:

$$\begin{aligned} S_1 = \big\{ & (m_{11}, m_{12}, m_{21}, m_{22}) \in \mathbb{F}_{2^m}^4 : \ m_{11} = 1, m_{12} \notin \{0,1\}, m_{21} = (m_{12}+1)^{-1}m_{12}, \\ & m_{22} \neq 0, m_{22} \neq m_{12}+1, m_{22} \neq (m_{12}+1)^{-1}m_{12}+1, m_{22} \neq (m_{12}+1)^{-1}m_{12}+m_{12} \big\}. \end{aligned}$$

Since $m_{11} = 1$ and $m_{21} = (m_{12}+1)^{-1}m_{12}$, then the problem of finding the cardinality of S_1 is reduced to find the count of two parameters m_{12} and m_{22}.

Now, since $m_{12} \in \mathbb{F}_{2^m} \setminus \{0,1\}$, we have $2^m - 2$ many choices for m_{12}.

Also, since $m_{22} \neq 0$, $m_{22} \neq m_{12}+1$, $m_{22} \neq (m_{12}+1)^{-1}m_{12}+1$, and $m_{22} \neq (m_{12}+1)^{-1}m_{12}+m_{12}$, we can say that $m_{22} \notin T_1$, where T_1 is defined as

$$T_1 = \big\{0, m_{12}+1, (m_{12}+1)^{-1}m_{12}+1, (m_{12}+1)^{-1}m_{12}+m_{12}\big\}.$$

We now demonstrate that the cardinality of T_1 is 4 for any $m_{12} \in \mathbb{F}_{2^m} \setminus \{0,1\}$. To establish this, we equate all pairs of elements in T_1 and solve for m_{12}. The resulting cases are as follows:

(i) $m_{12} + 1 = 0 \implies m_{12} = 1$,
(ii) $(m_{12}+1)^{-1}m_{12} + 1 = 0 \implies m_{12} = m_{12} + 1$,

(iii) $(m_{12}+1)^{-1}m_{12}+m_{12}=0 \implies m_{12}=0$,
(iv) $m_{12}+1=(m_{12}+1)^{-1}m_{12}+1 \implies m_{12}=0$,
(v) $m_{12}+1=(m_{12}+1)^{-1}m_{12}+m_{12} \implies m_{12}=m_{12}+1$,
(vi) $(m_{12}+1)^{-1}m_{12}+1=(m_{12}+1)^{-1}m_{12}+m_{12} \implies m_{12}=1$.

By analyzing these cases, we confirm that T_1 contains precisely four distinct elements. Hence, we have 2^m-4 many choices for m_{22}. Therefore, the cardinality of S_1 is $(2^m-2)(2^m-4)$.

Case II: $m_{11}\neq 1$. From (10) we have the following conditions on the parameters of M

$$\begin{aligned}&m_{11},m_{12},m_{21},m_{22}\in\mathbb{F}_{2^m}^*, m_{12}\neq m_{11}+1, m_{21}\neq m_{11}+1\\&m_{22}\neq m_{12}+1, m_{22}\neq m_{21}+1, m_{22}\neq m_{11}+m_{12}+m_{21}+1.\end{aligned}$$

The parameters of M also satisfy the following relation

$$\begin{aligned}&m_{11}m_{22}+m_{12}m_{21}+m_{11}+m_{12}+m_{21}+m_{22}=1\\ \implies\ & m_{22}=(m_{11}+1)^{-1}(m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1).\end{aligned} \tag{11}$$

Now, we will eliminate some restrictions on m_{22}. Since $m_{22}\neq 0$ and $m_{22}=(m_{11}+1)^{-1}(m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1)$, we have

$$\begin{aligned}&m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1\neq 0\\ \implies\ & m_{21}(m_{12}+1)\neq m_{11}+m_{12}+1.\end{aligned}$$

Also, $m_{22}\neq m_{12}+1$ implies that

$$\begin{aligned}&m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1\neq (m_{11}+1)(m_{12}+1)\\ \implies\ & m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1\neq m_{11}m_{12}+m_{11}+m_{12}+1\\ \implies\ & m_{21}(m_{12}+1)\neq m_{11}m_{12}.\end{aligned}$$

Also, when $m_{22}\neq m_{21}+1$ implies that

$$\begin{aligned}&m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1\neq (m_{11}+1)(m_{21}+1)\\ \implies\ & m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1\neq m_{11}m_{21}+m_{11}+m_{21}+1\\ \implies\ & m_{21}(m_{12}+m_{11})\neq m_{12}.\end{aligned}$$

Similarly, $m_{22}\neq m_{11}+m_{12}+m_{21}+1$ implies that

$$\begin{aligned}\implies\ & m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1\neq (m_{11}+1)(m_{11}+m_{12}+m_{21}+1)\\ \implies\ & m_{12}m_{21}\neq m_{11}(m_{11}+m_{12}+m_{21}+1)\\ \implies\ & m_{21}(m_{12}+m_{11})\neq m_{11}(m_{11}+m_{12}+1).\end{aligned}$$

Now, in this case, the number of all orthogonal MDS matrices of order 3 over $\mathbb{F}_{2^m}$ is equal to the cardinality of the set S_2, defined as:

$$
\begin{aligned}
S_2 = \Big\{&(m_{11}, m_{12}, m_{21}, m_{22}) \in \mathbb{F}_{2^m}^4 : \ m_{11} \notin \{0,1\}, \ m_{12} \neq 0, \ m_{12} \neq m_{11}+1, \ m_{21} \neq 0, \\
& m_{21} \neq m_{11}+1, \ m_{21}(m_{12}+1) \neq m_{11}+m_{12}+1, \ m_{21}(m_{12}+1) \neq m_{11}m_{12}, \\
& m_{21}(m_{12}+m_{11}) \neq m_{12}, \ m_{21}(m_{12}+m_{11}) \neq m_{11}(m_{11}+m_{12}+1), \\
& m_{22} = (m_{11}+1)^{-1}(m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1)\Big\}.
\end{aligned} \tag{12}
$$

Since $m_{22} = (m_{11}+1)^{-1}(m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1)$, then the problem of finding the cardinality of S_2 is reduced to find the count of three parameters m_{11}, m_{12} and m_{21}. For this, we will analyze two subcases further.

Subcase 1: $m_{12} = 1$. In this Subcase, the set S_2, given in (12), is reduced to

$$
\begin{aligned}
S_2 = \big\{&(m_{11}, m_{12}, m_{21}, m_{22}) \in \mathbb{F}_{2^m}^4 : \ m_{11} \notin \{0,1\}, \ m_{12} = 1, \ m_{21} \neq 0, \ m_{21} \neq m_{11}+1, \\
& m_{21} \neq (m_{11}+1)^{-1}, \ m_{21} \neq (m_{11}+1)^{-1}m_{11}^2, \ m_{22} = (m_{11}+1)^{-1}m_{11}\big\}.
\end{aligned}
$$

Now, since $m_{11} \in \mathbb{F}_{2^m} \setminus \{0,1\}$, we have $2^m - 2$ many choices for m_{11}.

Also since $m_{21} \neq 0$, $m_{21} \neq m_{11}+1$, $m_{21} \neq (m_{11}+1)^{-1}$, and $m_{21} \neq (m_{11}+1)^{-1}m_{11}^2$, we can say that $m_{21} \notin T_2$, where T_2 is defined as

$$
T_2 = \big\{0, m_{11}+1, (m_{11}+1)^{-1}, (m_{11}+1)^{-1}m_{11}^2\big\}.
$$

We now demonstrate that the cardinality of T_2 is 4 for any values of $m_{11} \in \mathbb{F}_{2^m} \setminus \{0,1\}$. To establish this, we equate all pairs of elements in T_1 and solve for m_{11}. By analyzing these six cases, we confirm that T_2 contains precisely four distinct elements. Thus, for m_{21}, we have $2^m - 4$ many choices over $\mathbb{F}_{2^m}$.

Hence, in this Subcase, the cardinality of S_2 is $(2^m-2)(2^m-4)$.

Subcase 2: $m_{12} \neq 1$. In this subcase, we will analyze two subcases further.

Subcase 2.1: $m_{11} = m_{12}$. In this Subcase, the set S_2, given in (12), is reduced to

$$
\begin{aligned}
S_2 = \big\{&(m_{11}, m_{12}, m_{21}, m_{22}) \in \mathbb{F}_{2^m}^4 : \ m_{11} \notin \{0,1\}, \ m_{12} = m_{11}, \ m_{21} \neq 0, \\
& m_{21} \neq m_{11}+1, \ m_{21} \neq (m_{11}+1)^{-1}, \ m_{21} \neq (m_{11}+1)^{-1}m_{11}^2, \\
& m_{22} = (m_{11}+1)^{-1}(m_{11}m_{21}+m_{21}+1)\big\}.
\end{aligned}
$$

Now, since $m_{11} \in \mathbb{F}_{2^m} \setminus \{0,1\}$, we have $2^m - 2$ many choices for m_{11}.

Also, we have $m_{21} \neq 0$, $m_{21} \neq m_{11}+1$, $m_{21} \neq (m_{11}+1)^{-1}$, and $m_{21} \neq (m_{11}+1)^{-1}m_{11}^2$. Therefore, by the similar analysis done for Subcase 1, we can conclude that we have $2^m - 4$ many choices for m_{21}.

Hence, in Subcase 2.1, the cardinality of S_2 is $(2^m-2)(2^m-4)$.

Subcase 2.2: $m_{11} \neq m_{12}$. In this Subcase, the set S_2, given in (12), is reduced to

$$S_2 = \big\{(m_{11}, m_{12}, m_{21}, m_{22}) \in \mathbb{F}_{2^m}^4 : \ m_{11}, m_{12} \notin \{0,1\},\ m_{12} \neq m_{11},\ m_{12} \neq m_{11}+1,\\ m_{21} \neq 0,\ m_{21} \neq m_{11}+1,\ m_{21} \neq (m_{12}+1)^{-1}(m_{11}+m_{12}+1),\\ m_{21} \neq (m_{12}+1)^{-1}m_{11}m_{12},\ m_{21} \neq (m_{11}+m_{12})^{-1}m_{12},\\ m_{21} \neq m_{11}(m_{11}+m_{12})^{-1}(m_{11}+m_{12}+1),\\ m_{22} = (m_{11}+1)^{-1}(m_{12}m_{21}+m_{11}+m_{12}+m_{21}+1)\big\}.$$

Now, since $m_{11} \in \mathbb{F}_{2^m} \setminus \{0,1\}$, we have $2^m - 2$ many choices for m_{11}.

Also since $m_{12} \in \mathbb{F}_{2^m} \setminus \{0,1\}$, $m_{12} \neq m_{11}$, and $m_{12} \neq m_{11}+1$, for m_{12}, we have $2^m - 4$ many choices.

Also since $m_{21} \neq 0$, $m_{21} \neq m_{11}+1$, $m_{21} \neq (m_{12}+1)^{-1}(m_{11}+m_{12}+1)$, $m_{21} \neq (m_{12}+1)^{-1}m_{11}m_{12}$, $m_{21} \neq (m_{11}+m_{12})^{-1}m_{12}$, and $m_{21} \neq m_{11}(m_{11}+m_{12})^{-1}(m_{11}+m_{12}+1)$, we can say that $m_{21} \notin T_3$, where T_3 is defined as

$$T_3 = \{0, m_{11}+1, (m_{12}+1)^{-1}(m_{11}+m_{12}+1), (m_{12}+1)^{-1}m_{11}m_{12},\\ (m_{11}+m_{12})^{-1}m_{12}, m_{11}(m_{11}+m_{12})^{-1}(m_{11}+m_{12}+1)\}.$$

We now demonstrate that the cardinality of T_3 is 6 for any values of $m_{11} \notin \mathbb{F}_{2^m} \setminus \{0,1\}$ and $m_{12} \notin \{0, 1, m_{11}, m_{11}+1\}$. To establish this, we equate all pairs of elements in T_3 and solve for m_{11} or m_{12}. By analyzing these 15 cases, we can say that T_3 contains precisely six elements. Therefore, we have $2^m - 6$ many choices for m_{21}.

Hence, in Subcase 2.2, the cardinality of S_2 is $(2^m-2)(2^m-4)(2^m-6)$.

Therefore, in Subcase 2, the cardinality of S_2 is given by

$$(2^m-2)(2^m-4) + (2^m-2)(2^m-4)(2^m-6)\\ = (2^m-2)(2^m-4)(2^m-5).$$

The cardinality of S_2 in **Case II** is determined by whether $m_{12} = 1$ (Subcase 1) or $m_{12} \neq 1$ (Subcase 2), and is given by

$$(2^m-2)(2^m-4) + (2^m-2)(2^m-4)(2^m-5)\\ = (2^m-2)(2^m-4)^2.$$

Finally, by analyzing **Case I** and **Case II**, we can conclude that the total number of orthogonal MDS matrices of order 3 over $\mathbb{F}_{2^m}$ is

$$(2^m-2)(2^m-4) + (2^m-2)(2^m-4)^2\\ = (2^m-2)(2^m-3)(2^m-4).$$

This conclude the proof. □

The number of all 3×3 orthogonal MDS matrices is $(2^m-2)(2^m-3)(2^m-4)$, as demonstrated in Theorem 13. Hence, from Theorem 7, the number of all 3×3

semi-orthogonal representative MDS matrices of the form M_1 is $(2^m-2)(2^m-3)(2^m-4)$. By the definition of a semi-orthogonal matrix, for any two non-singular diagonal matrices D_1 and D_2, if M_1 is semi-orthogonal, then $M = \Phi(D_1, D_2, M_1)$ is also a semi-orthogonal matrix. Hence, choices for D_1 and D_2 for M to be a semi-orthogonal matrix are $(2^m-1)^5$, therefore, the number of all 3×3 semi-orthogonal MDS matrices is $(2^m-1)^5(2^m-2)(2^m-3)(2^m-4)$. We formally present this result below.

Theorem 14. *For $m \geq 3$, the number of semi-orthogonal MDS matrices of order 3 over $\mathbb{F}_{2^m}$ is $(2^m-1)^5(2^m-2)(2^m-3)(2^m-4)$.*

Remark 5. We note that in a recent work [16], the authors derived a formula for counting 3×3 semi-orthogonal MDS matrices over $\mathbb{F}_{2^m}$. We derive the general structure of $n\times n$ orthogonal matrices over $\mathbb{F}_{2^m}$, which yields the formula $(2^m-2)(2^m-3)(2^m-4)$ for 3×3 orthogonal MDS matrices. The structural interconnections we establish in Theorem 7 between semi-orthogonal and orthogonal matrices provide a theoretical link between our enumeration and their result.

From Theorem 12, we know that any 4×4 orthogonal matrix over $\mathbb{F}_{2^m}$ can be expressed in the following form:

$$\begin{pmatrix} m_{11} & m_{12} & m_{13} & b_1+1 \\ m_{21} & m_{22} & m_{23} & b_2+1 \\ m_{31} & m_{32} & m_{33} & b_3+1 \\ c_1+1 & c_2+1 & c_3+1 & b_1+b_2+b_3 \end{pmatrix}, \tag{13}$$

where $b_i = \sum_{j=1}^{3} m_{ij}$, $c_j = \sum_{i=1}^{3} m_{ij}$, $1 \leq i, j \leq 3$ and m_{ij}'s satisfy the following equations for $1 \leq k < l \leq 3$

$$\sum_{i=1}^{3}\sum_{j=1, j\neq i}^{3} m_{ki}m_{lj} + b_k + b_l = 1$$

$$\sum_{i=1}^{3}\sum_{j=1, j\neq i}^{3} m_{ik}m_{jl} + c_k + c_l = 1.$$

Now, we are ready to get a count of the 4×4 orthogonal MDS matrices over $\mathbb{F}_{2^m}$. The result is given in Table 2. Note that because of the large search space involved, we are unable to offer the count of all 4×4 orthogonal MDS matrices over $\mathbb{F}_{2^m}$ for $m \geq 5$. Nevertheless, no explicit count is currently available for all 4×4 orthogonal MDS matrices. Hence, an explicit formula for counting the orthogonal MDS matrices of order $n \geq 4$ could be a possible direction for future research.

Remark 6. It is worth noting that there is an additional advantage to constructing an orthogonal MDS matrix. We know that if all of the entries in the inverse of a 4×4 non-singular matrix are non-zero, then all of its 3×3 sub-matrices are also non-singular (in this case, $M^{-1} = M^T$). Therefore, to confirm the MDS property of the orthogonal matrix of order 4, we need to inspect sub-matrices of M of order 1 and 2.

Since 4×4 matrices are most commonly used in the design of block ciphers and hash functions, we focus on finding efficient orthogonal MDS matrices of order 4. To do so, we use the general form given in (13) to identify the lightest orthogonal MDS matrices. In the past, it was widely believed that implementing the multiplication of finite field elements with low Hamming weights incurred lower hardware costs. However, in 2014, the authors of [13] proposed an approach for estimating implementation costs by counting the number of XOR gates (d-XOR gates) required to implement the field element based on the multiplicative matrix of the element.

We adopt this metric to identify lightweight orthogonal MDS matrices of order 4 over $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^4}$. We found that orthogonal MDS matrices of order 4 achieve the lowest d-XOR count of 64 over $\mathbb{F}_{2^3}$, with 144 such matrices exhibiting this optimal count. These matrices are provided in Appendix A. Similarly, we observed that orthogonal MDS matrices of order 4 achieve the lowest d-XOR count of 72 over $\mathbb{F}_{2^4}$, with 144 matrices that have the lowest d-XOR count. These matrices are listed in Appendix B.

Table 4. Comparison of the count of 3×3 MDS matrices with various properties

	IMDS	SIMDS	OMDS	SOMDS	SISOMDS
$\mathbb{F}_{2^3}$	$7^2 \times 24$	$7^5 \times 24$	120	$7^5 \times 120$	$7^5 \times 24$
$\mathbb{F}_{2^4}$	$15^2 \times 168$	$15^5 \times 168$	2184	$15^5 \times 2184$	$15^5 \times 168$
$\mathbb{F}_{2^5}$	$31^2 \times 840$	$31^5 \times 840$	24360	$31^5 \times 24360$	$31^5 \times 840$
$\mathbb{F}_{2^6}$	$63^2 \times 3720$	$63^5 \times 3720$	226920	$63^5 \times 226920$	$63^5 \times 3720$
$\mathbb{F}_{2^7}$	$127^2 \times 15624$	$127^5 \times 15624$	1953000	$127^5 \times 1953000$	$127^5 \times 15624$
$\mathbb{F}_{2^8}$	$255^2 \times 64008$	$255^5 \times 64008$	16194024	$255^5 \times 16194024$	$255^5 \times 64008$

Table 5. Comparison of the count of 4×4 MDS matrices with various properties [1]

	IMDS	SIMDS	OMDS	SOMDS	SISOMDS
$\mathbb{F}_{2^3}$	$7^3 \times 48$	$7^7 \times 48$	720	$7^7 \times 720$	$7^7 \times 48$
$\mathbb{F}_{2^4}$	$15^3 \times 71856$	$15^7 \times 71856$	1147440	$15^7 \times 1147440$	$15^7 \times 11088$
$\mathbb{F}_{2^5}$	$31^3 \times 10188240$	$31^7 \times 10188240$			
$\mathbb{F}_{2^6}$	$63^3 \times 612203760$	$63^7 \times 612203760$			
$\mathbb{F}_{2^7}$	$127^3 \times 26149708368$	$127^7 \times 26149708368$			
$\mathbb{F}_{2^8}$	$255^3 \times 961006331376$	$255^7 \times 961006331376$			

[1] The abbreviations are as follows. IMDS: Involutory MDS, SIMDS: Semi-involutory MDS, OMDS: Orthogonal MDS, SOMDS: Semi-orthogonal MDS, and SISOMDS: Semi-involutory and semi-orthogonal MDS. The same abbreviations apply to Table 4.

5 Conclusion

This paper presents a study of the structural relationships between semi-involutory and involutory matrices, as well as between semi-orthogonal and orthogonal matrices. We show that these relationships allow us to derive the enumeration of semi-involutory MDS matrices from the count of involutory ones, and vice versa. A similar correspondence is demonstrated for the semi-orthogonal and orthogonal cases. Leveraging these results, we provide a simplified derivation of the formula for counting 3×3 semi-involutory MDS matrices. Additionally, we establish explicit formulas for enumerating 3×3 orthogonal and semi-orthogonal MDS matrices over $\mathbb{F}_{2^m}$. We also characterize the class of matrices that simultaneously satisfy both the semi-involutory and semi-orthogonal properties. Using this characterization, we prove that the number of 3×3 MDS matrices possessing both properties is identical to the count of 3×3 semi-involutory MDS matrices over $\mathbb{F}_{2^m}$. Finally, we extend our analysis to 4×4 matrices by determining the number of semi-involutory MDS matrices over $\mathbb{F}_{2^m}$ for $m = 3, 4, \ldots, 8$, as well as the counts of orthogonal and semi-orthogonal MDS matrices over $\mathbb{F}_{2^m}$ for $m = 3, 4$.

References

1. PSLM Barreto and M Simplicio. Curupira, a block cipher for constrained platforms. *25th Brazilian Symposium on Computer Networks and Distributed Systems (SBRC)*, 1:61–74, 2007.
2. Tapas Chatterjee and Ayantika Laha. A note on semi-orthogonal (G-matrix) and semi-involutory MDS matrices. *Finite Fields and Their Applications*, 92:102279, 2023.
3. Tapas Chatterjee and Ayantika Laha. A Characterization of Semi-Involutory MDS Matrices, 2024. https://arxiv.org/abs/2406.12842.
4. Tapas Chatterjee and Ayantika Laha. A note on MDS property of Circulant Matrices, 2024. https://arxiv.org/abs/2406.16973.
5. Gi-Sang Cheon, Bryan Curtis, and Hana Kim. Semi-involutory matrices and signed self-inverse. *Linear Algebra and its Applications*, 622:294–315, 2021.
6. Sébastien Duval and Gaëtan Leurent. MDS Matrices with Lightweight Circuits. *IACR Trans. Symmetric Cryptol.*, 2018(2):48–78, 2018.
7. Miroslav Fiedler and Frank J. Hall. G-matrices. *Linear Algebra and its Applications*, 436(3):731–741, 2012.
8. Kishan Chand Gupta, Sumit Kumar Pandey, Indranil Ghosh Ray, and Susanta Samanta. Cryptographically significant MDS matrices over finite fields: A brief survey and some generalized results. *Advances in Mathematics of Communications*, 13(4):779–843, 2019.
9. Kishan Chand Gupta, Sumit Kumar Pandey, and Susanta Samanta. On the Direct Construction of MDS and Near-MDS Matrices, 2023. https://arxiv.org/abs/2306.12848.
10. Kishan Chand Gupta and Indranil Ghosh Ray. On constructions of involutory MDS matrices. In *International Conference on Cryptology in Africa*, pages 43–60. Springer, 2013.

11. Kishan Chand Gupta and Indranil Ghosh Ray. Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. *Cryptography and Communications*, 7:257–287, 2015.
12. Gülsüm Gözde Güzel, Muharrem Tolga Sakalli, Sedat Akleylek, Vincent Rijmen, and Yasemin Çengellenmiş. A new matrix form to generate all 3×3 involutory MDS matrices over $\mathbb{F}_{2^m}$. *Information Processing Letters*, 147:61–68, 2019.
13. 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*, pages 433–450, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.
14. Yogesh Kumar, P. R. Mishra, Susanta Samanta, and Atul Gaur. A systematic construction approach for all 4×4 involutory MDS matrices. *Journal of Applied Mathematics and Computing*, 70(5):4677–4697, 2024.
15. Yogesh Kumar, Prasanna Raghaw Mishra, Susanta Samanta, Kishan Chand Gupta, and Atul Gaur. Construction of all MDS and involutory MDS matrices. *Advances in Mathematics of Communications*, 19(3):922–941, 2025.
16. Yogesh Kumar, Susanta Samanta, PR Mishra, and Atul Gaur. On the study of semi-involutory and semi-orthogonal matrices. *Finite Fields and Their Applications*, 110:102730, 2026.
17. Jérôme Lacan and Jérôme Fimes. A Construction of Matrices with No Singular Square Submatrices. In Gary L. Mullen, Alain Poli, and Henning Stichtenoth, editors, *Finite Fields and Applications*, pages 145–147, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.
18. Shun Li, Siwei Sun, Chaoyun Li, Zihao Wei, and Lei Hu. Constructing Low-latency Involutory MDS Matrices with Lightweight Circuits. *IACR Transactions on Symmetric Cryptology*, pages 84–117, 03 2019.
19. Shun Li, Siwei Sun, Danping Shi, Chaoyun Li, and Lei Hu. Lightweight Iterative MDS Matrices: How Small Can We Go? *IACR Trans. Symmetric Cryptol.*, 2019(4):147–170, 2019.
20. Meicheng Liu and Siang Meng Sim. Lightweight MDS Generalized Circulant Matrices. In Thomas Peyrin, editor, *Fast Software Encryption*, pages 101–120, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.
21. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error Correcting Codes*. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.
22. Meltem Kurt Pehlivanoğlu, Muharrem Tolga Sakalli, Sedat Akleylek, Nevcihan Duru, and Vincent Rijmen. Generalisation of Hadamard matrix to generate involutory MDS matrices for lightweight cryptography. *IET Information Security*, 12(4):348–355, 2018.
23. Ron M. Roth and Abraham Lempel. On MDS codes via Cauchy matrices. *IEEE Transactions on Information Theory*, 35(6):1314–1319, 1989.
24. Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Behnaz Omoomi. On construction of Involutory MDS Matrices from Vandermonde Matrices in $GF(2^q)$. *Designs, Codes and Cryptography*, 64(3):287–308, sep 2012.
25. Mahdi Sajadieh and Mohsen Mousavi. Construction of MDS matrices from generalized Feistel structures. *Designs, Codes and Cryptography*, 89(7):1433–1452, 2021.
26. C. E. Shannon. Communication Theory of Secrecy Systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.
27. Siang Meng Sim, Khoongming Khoo, Frédérique Oggier, and Thomas Peyrin. Lightweight MDS Involution Matrices. In Gregor Leander, editor, *Fast Software Encryption*, pages 471–493, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

28. A. F. Webster and S. E. Tavares. On the Design of S-Boxes. In Hugh C. Williams, editor, *Advances in Cryptology — CRYPTO '85 Proceedings*, pages 523–534, Berlin, Heidelberg, 1986. Springer Berlin Heidelberg.
29. Zejun Xiang, Xiangyoung Zeng, Da Lin, Zhenzhen Bao, and Shasha Zhang. Optimizing Implementations of Linear Layers. *IACR Transactions on Symmetric Cryptology*, pages 120–145, 2020.
30. Lijing Zhou, Licheng Wang, and Yiru Sun. On the Construction of Lightweight Orthogonal MDS Matrices. Cryptology ePrint Archive, Paper 2017/371, 2017.

A The 4×4 orthogonal MDS matrices with optimal d-XOR count 64 over $\mathbb{F}_{2^3}/0\text{x}b$

The tuples in the following are represented as $(m_{11}, m_{12}, m_{13}, m_{21}, m_{22}, m_{23}, m_{31}, m_{32}, m_{33})$, where m_{ij} $(1 \le i, j \le 3)$ are defined by equation (13).

$(1_x,2_x,4_x,2_x,1_x,6_x,4_x,6_x,1_x)$, $(1_x,2_x,4_x,2_x,1_x,6_x,6_x,4_x,2_x)$, $(1_x,2_x,4_x,4_x,6_x,1_x,2_x,1_x,6_x)$
$(1_x,2_x,4_x,4_x,6_x,1_x,6_x,4_x,2_x)$, $(1_x,2_x,4_x,6_x,4_x,2_x,2_x,1_x,6_x)$, $(1_x,2_x,4_x,6_x,4_x,2_x,4_x,6_x,1_x)$
$(1_x,2_x,6_x,2_x,1_x,4_x,4_x,6_x,2_x)$, $(1_x,2_x,6_x,2_x,1_x,4_x,6_x,4_x,1_x)$, $(1_x,2_x,6_x,4_x,6_x,2_x,2_x,1_x,4_x)$
$(1_x,2_x,6_x,4_x,6_x,2_x,6_x,4_x,1_x)$, $(1_x,2_x,6_x,6_x,4_x,1_x,2_x,1_x,4_x)$, $(1_x,2_x,6_x,6_x,4_x,1_x,4_x,6_x,2_x)$
$(1_x,4_x,2_x,2_x,6_x,1_x,4_x,1_x,6_x)$, $(1_x,4_x,2_x,2_x,6_x,1_x,6_x,2_x,4_x)$, $(1_x,4_x,2_x,4_x,1_x,6_x,2_x,6_x,1_x)$
$(1_x,4_x,2_x,4_x,1_x,6_x,6_x,2_x,4_x)$, $(1_x,4_x,2_x,6_x,2_x,4_x,2_x,6_x,1_x)$, $(1_x,4_x,2_x,6_x,2_x,4_x,4_x,1_x,6_x)$
$(1_x,4_x,6_x,2_x,6_x,4_x,4_x,1_x,2_x)$, $(1_x,4_x,6_x,2_x,6_x,4_x,6_x,2_x,1_x)$, $(1_x,4_x,6_x,4_x,1_x,2_x,2_x,6_x,4_x)$
$(1_x,4_x,6_x,4_x,1_x,2_x,6_x,2_x,1_x)$, $(1_x,4_x,6_x,6_x,2_x,1_x,2_x,6_x,4_x)$, $(1_x,4_x,6_x,6_x,2_x,1_x,4_x,1_x,2_x)$
$(1_x,6_x,2_x,2_x,4_x,1_x,4_x,2_x,6_x)$, $(1_x,6_x,2_x,2_x,4_x,1_x,6_x,1_x,4_x)$, $(1_x,6_x,2_x,4_x,2_x,6_x,2_x,4_x,1_x)$
$(1_x,6_x,2_x,4_x,2_x,6_x,6_x,1_x,4_x)$, $(1_x,6_x,2_x,6_x,1_x,4_x,2_x,4_x,1_x)$, $(1_x,6_x,2_x,6_x,1_x,4_x,4_x,2_x,6_x)$
$(1_x,6_x,4_x,2_x,4_x,6_x,4_x,2_x,1_x)$, $(1_x,6_x,4_x,2_x,4_x,6_x,6_x,1_x,2_x)$, $(1_x,6_x,4_x,4_x,2_x,1_x,2_x,4_x,6_x)$
$(1_x,6_x,4_x,4_x,2_x,1_x,6_x,1_x,2_x)$, $(1_x,6_x,4_x,6_x,1_x,2_x,2_x,4_x,6_x)$, $(1_x,6_x,4_x,6_x,1_x,2_x,4_x,2_x,1_x)$
$(2_x,1_x,4_x,1_x,2_x,6_x,4_x,6_x,2_x)$, $(2_x,1_x,4_x,1_x,2_x,6_x,6_x,4_x,1_x)$, $(2_x,1_x,4_x,4_x,6_x,2_x,1_x,2_x,6_x)$
$(2_x,1_x,4_x,4_x,6_x,2_x,6_x,4_x,1_x)$, $(2_x,1_x,4_x,6_x,4_x,1_x,1_x,2_x,6_x)$, $(2_x,1_x,4_x,6_x,4_x,1_x,4_x,6_x,2_x)$
$(2_x,1_x,6_x,1_x,2_x,4_x,4_x,6_x,1_x)$, $(2_x,1_x,6_x,1_x,2_x,4_x,6_x,4_x,2_x)$, $(2_x,1_x,6_x,4_x,6_x,1_x,1_x,2_x,4_x)$
$(2_x,1_x,6_x,4_x,6_x,1_x,6_x,4_x,2_x)$, $(2_x,1_x,6_x,6_x,4_x,2_x,1_x,2_x,4_x)$, $(2_x,1_x,6_x,6_x,4_x,2_x,4_x,6_x,1_x)$
$(2_x,4_x,1_x,1_x,6_x,2_x,4_x,2_x,6_x)$, $(2_x,4_x,1_x,1_x,6_x,2_x,6_x,1_x,4_x)$, $(2_x,4_x,1_x,4_x,2_x,6_x,1_x,6_x,2_x)$
$(2_x,4_x,1_x,4_x,2_x,6_x,6_x,1_x,4_x)$, $(2_x,4_x,1_x,6_x,1_x,4_x,1_x,6_x,2_x)$, $(2_x,4_x,1_x,6_x,1_x,4_x,4_x,2_x,6_x)$
$(2_x,4_x,6_x,1_x,6_x,4_x,4_x,2_x,1_x)$, $(2_x,4_x,6_x,1_x,6_x,4_x,6_x,1_x,2_x)$, $(2_x,4_x,6_x,4_x,2_x,1_x,1_x,6_x,4_x)$
$(2_x,4_x,6_x,4_x,2_x,1_x,6_x,1_x,2_x)$, $(2_x,4_x,6_x,6_x,1_x,2_x,1_x,6_x,4_x)$, $(2_x,4_x,6_x,6_x,1_x,2_x,4_x,2_x,1_x)$
$(2_x,6_x,1_x,1_x,4_x,2_x,4_x,1_x,6_x)$, $(2_x,6_x,1_x,1_x,4_x,2_x,6_x,2_x,4_x)$, $(2_x,6_x,1_x,4_x,1_x,6_x,1_x,4_x,2_x)$
$(2_x,6_x,1_x,4_x,1_x,6_x,6_x,2_x,4_x)$, $(2_x,6_x,1_x,6_x,2_x,4_x,1_x,4_x,2_x)$, $(2_x,6_x,1_x,6_x,2_x,4_x,4_x,1_x,6_x)$
$(2_x,6_x,4_x,1_x,4_x,6_x,4_x,1_x,2_x)$, $(2_x,6_x,4_x,1_x,4_x,6_x,6_x,2_x,1_x)$, $(2_x,6_x,4_x,4_x,1_x,2_x,1_x,4_x,6_x)$
$(2_x,6_x,4_x,4_x,1_x,2_x,6_x,2_x,1_x)$, $(2_x,6_x,4_x,6_x,2_x,1_x,1_x,4_x,6_x)$, $(2_x,6_x,4_x,6_x,2_x,1_x,4_x,1_x,2_x)$
$(4_x,1_x,2_x,1_x,4_x,6_x,2_x,6_x,4_x)$, $(4_x,1_x,2_x,1_x,4_x,6_x,6_x,2_x,1_x)$, $(4_x,1_x,2_x,2_x,6_x,4_x,1_x,4_x,6_x)$
$(4_x,1_x,2_x,2_x,6_x,4_x,6_x,2_x,1_x)$, $(4_x,1_x,2_x,6_x,2_x,1_x,1_x,4_x,6_x)$, $(4_x,1_x,2_x,6_x,2_x,1_x,2_x,6_x,4_x)$
$(4_x,1_x,6_x,1_x,4_x,2_x,2_x,6_x,1_x)$, $(4_x,1_x,6_x,1_x,4_x,2_x,6_x,2_x,4_x)$, $(4_x,1_x,6_x,2_x,6_x,1_x,1_x,4_x,2_x)$
$(4_x,1_x,6_x,2_x,6_x,1_x,6_x,2_x,4_x)$, $(4_x,1_x,6_x,6_x,2_x,4_x,1_x,4_x,2_x)$, $(4_x,1_x,6_x,6_x,2_x,4_x,2_x,6_x,1_x)$
$(4_x,2_x,1_x,1_x,6_x,4_x,2_x,4_x,6_x)$, $(4_x,2_x,1_x,1_x,6_x,4_x,6_x,1_x,2_x)$, $(4_x,2_x,1_x,2_x,4_x,6_x,1_x,6_x,4_x)$
$(4_x,2_x,1_x,2_x,4_x,6_x,6_x,1_x,2_x)$, $(4_x,2_x,1_x,6_x,1_x,2_x,1_x,6_x,4_x)$, $(4_x,2_x,1_x,6_x,1_x,2_x,2_x,4_x,6_x)$
$(4_x,2_x,6_x,1_x,6_x,2_x,2_x,4_x,1_x)$, $(4_x,2_x,6_x,1_x,6_x,2_x,6_x,1_x,4_x)$, $(4_x,2_x,6_x,2_x,4_x,1_x,1_x,6_x,2_x)$
$(4_x,2_x,6_x,2_x,4_x,1_x,6_x,1_x,4_x)$, $(4_x,2_x,6_x,6_x,1_x,4_x,1_x,6_x,2_x)$, $(4_x,2_x,6_x,6_x,1_x,4_x,2_x,4_x,1_x)$
$(4_x,6_x,1_x,1_x,2_x,4_x,2_x,1_x,6_x)$, $(4_x,6_x,1_x,1_x,2_x,4_x,6_x,4_x,2_x)$, $(4_x,6_x,1_x,2_x,1_x,6_x,1_x,2_x,4_x)$

$(4_x, 6_x, 1_x, 2_x, 1_x, 6_x, 6_x, 4_x, 2_x)$, $(4_x, 6_x, 1_x, 6_x, 4_x, 2_x, 1_x, 2_x, 4_x)$, $(4_x, 6_x, 1_x, 6_x, 4_x, 2_x, 2_x, 1_x, 6_x)$
$(4_x, 6_x, 2_x, 1_x, 2_x, 6_x, 2_x, 1_x, 4_x)$, $(4_x, 6_x, 2_x, 1_x, 2_x, 6_x, 6_x, 4_x, 1_x)$, $(4_x, 6_x, 2_x, 2_x, 1_x, 4_x, 1_x, 2_x, 6_x)$
$(4_x, 6_x, 2_x, 2_x, 1_x, 4_x, 6_x, 4_x, 1_x)$, $(4_x, 6_x, 2_x, 6_x, 4_x, 1_x, 1_x, 2_x, 6_x)$, $(4_x, 6_x, 2_x, 6_x, 4_x, 1_x, 2_x, 1_x, 4_x)$
$(6_x, 1_x, 2_x, 1_x, 6_x, 4_x, 2_x, 4_x, 6_x)$, $(6_x, 1_x, 2_x, 1_x, 6_x, 4_x, 4_x, 2_x, 1_x)$, $(6_x, 1_x, 2_x, 2_x, 4_x, 6_x, 1_x, 6_x, 4_x)$
$(6_x, 1_x, 2_x, 2_x, 4_x, 6_x, 4_x, 2_x, 1_x)$, $(6_x, 1_x, 2_x, 4_x, 2_x, 1_x, 1_x, 6_x, 4_x)$, $(6_x, 1_x, 2_x, 4_x, 2_x, 1_x, 2_x, 4_x, 6_x)$
$(6_x, 1_x, 4_x, 1_x, 6_x, 2_x, 2_x, 4_x, 1_x)$, $(6_x, 1_x, 4_x, 1_x, 6_x, 2_x, 4_x, 2_x, 6_x)$, $(6_x, 1_x, 4_x, 2_x, 4_x, 1_x, 1_x, 6_x, 2_x)$
$(6_x, 1_x, 4_x, 2_x, 4_x, 1_x, 4_x, 2_x, 6_x)$, $(6_x, 1_x, 4_x, 4_x, 2_x, 6_x, 1_x, 6_x, 2_x)$, $(6_x, 1_x, 4_x, 4_x, 2_x, 6_x, 2_x, 4_x, 1_x)$
$(6_x, 2_x, 1_x, 1_x, 4_x, 6_x, 2_x, 6_x, 4_x)$, $(6_x, 2_x, 1_x, 1_x, 4_x, 6_x, 4_x, 1_x, 2_x)$, $(6_x, 2_x, 1_x, 2_x, 6_x, 4_x, 1_x, 4_x, 6_x)$
$(6_x, 2_x, 1_x, 2_x, 6_x, 4_x, 4_x, 1_x, 2_x)$, $(6_x, 2_x, 1_x, 4_x, 1_x, 2_x, 1_x, 4_x, 6_x)$, $(6_x, 2_x, 1_x, 4_x, 1_x, 2_x, 2_x, 6_x, 4_x)$
$(6_x, 2_x, 4_x, 1_x, 4_x, 2_x, 2_x, 6_x, 1_x)$, $(6_x, 2_x, 4_x, 1_x, 4_x, 2_x, 4_x, 1_x, 6_x)$, $(6_x, 2_x, 4_x, 2_x, 6_x, 1_x, 1_x, 4_x, 2_x)$
$(6_x, 2_x, 4_x, 2_x, 6_x, 1_x, 4_x, 1_x, 6_x)$, $(6_x, 2_x, 4_x, 4_x, 1_x, 6_x, 1_x, 4_x, 2_x)$, $(6_x, 2_x, 4_x, 4_x, 1_x, 6_x, 2_x, 6_x, 1_x)$
$(6_x, 4_x, 1_x, 1_x, 2_x, 6_x, 2_x, 1_x, 4_x)$, $(6_x, 4_x, 1_x, 1_x, 2_x, 6_x, 4_x, 6_x, 2_x)$, $(6_x, 4_x, 1_x, 2_x, 1_x, 4_x, 1_x, 2_x, 6_x)$
$(6_x, 4_x, 1_x, 2_x, 1_x, 4_x, 4_x, 6_x, 2_x)$, $(6_x, 4_x, 1_x, 4_x, 6_x, 2_x, 1_x, 2_x, 6_x)$, $(6_x, 4_x, 1_x, 4_x, 6_x, 2_x, 2_x, 1_x, 4_x)$
$(6_x, 4_x, 2_x, 1_x, 2_x, 4_x, 2_x, 1_x, 6_x)$, $(6_x, 4_x, 2_x, 1_x, 2_x, 4_x, 4_x, 6_x, 1_x)$, $(6_x, 4_x, 2_x, 2_x, 1_x, 6_x, 1_x, 2_x, 4_x)$
$(6_x, 4_x, 2_x, 2_x, 1_x, 6_x, 4_x, 6_x, 1_x)$, $(6_x, 4_x, 2_x, 4_x, 6_x, 1_x, 1_x, 2_x, 4_x)$, $(6_x, 4_x, 2_x, 4_x, 6_x, 1_x, 2_x, 1_x, 6_x)$

B The 4 × 4 orthogonal MDS matrices with optimal d-XOR count 72 over $\mathbb{F}_{2^4}/0x13$

The tuples in the following are represented as $(m_{11}, m_{12}, m_{13}, m_{21}, m_{22}, m_{23}, m_{31}, m_{32}, m_{33})$, where m_{ij} $(1 \leq i, j \leq 3)$ are defined by equation (13).

$(1_x, 4_x, 9_x, 4_x, 1_x, d_x, 9_x, d_x, 1_x)$, $(1_x, 4_x, 9_x, 4_x, 1_x, d_x, d_x, 9_x, 4_x)$, $(1_x, 4_x, 9_x, 9_x, d_x, 1_x, 4_x, 1_x, d_x)$
$(1_x, 4_x, 9_x, 9_x, d_x, 1_x, d_x, 9_x, 4_x)$, $(1_x, 4_x, 9_x, d_x, 9_x, 4_x, 4_x, 1_x, d_x)$, $(1_x, 4_x, 9_x, d_x, 9_x, 4_x, 9_x, d_x, 1_x)$
$(1_x, 4_x, d_x, 4_x, 1_x, 9_x, 9_x, d_x, 4_x)$, $(1_x, 4_x, d_x, 4_x, 1_x, 9_x, d_x, 9_x, 1_x)$, $(1_x, 4_x, d_x, 9_x, d_x, 4_x, 4_x, 1_x, 9_x)$
$(1_x, 4_x, d_x, 9_x, d_x, 4_x, d_x, 9_x, 1_x)$, $(1_x, 4_x, d_x, d_x, 9_x, 1_x, 4_x, 1_x, 9_x)$, $(1_x, 4_x, d_x, d_x, 9_x, 1_x, 9_x, d_x, 4_x)$
$(1_x, 9_x, 4_x, 4_x, d_x, 1_x, 9_x, 1_x, d_x)$, $(1_x, 9_x, 4_x, 4_x, d_x, 1_x, d_x, 4_x, 9_x)$, $(1_x, 9_x, 4_x, 9_x, 1_x, d_x, 4_x, d_x, 1_x)$
$(1_x, 9_x, 4_x, 9_x, 1_x, d_x, d_x, 4_x, 9_x)$, $(1_x, 9_x, 4_x, d_x, 4_x, 9_x, 4_x, d_x, 1_x)$, $(1_x, 9_x, 4_x, d_x, 4_x, 9_x, 9_x, 1_x, d_x)$
$(1_x, 9_x, d_x, 4_x, d_x, 9_x, 9_x, 1_x, 4_x)$, $(1_x, 9_x, d_x, 4_x, d_x, 9_x, d_x, 4_x, 1_x)$, $(1_x, 9_x, d_x, 9_x, 1_x, 4_x, 4_x, d_x, 9_x)$
$(1_x, 9_x, d_x, 9_x, 1_x, 4_x, d_x, 4_x, 1_x)$, $(1_x, 9_x, d_x, d_x, 4_x, 1_x, 4_x, d_x, 9_x)$, $(1_x, 9_x, d_x, d_x, 4_x, 1_x, 9_x, 1_x, 4_x)$
$(1_x, d_x, 4_x, 4_x, 9_x, 1_x, 9_x, 4_x, d_x)$, $(1_x, d_x, 4_x, 4_x, 9_x, 1_x, d_x, 1_x, 9_x)$, $(1_x, d_x, 4_x, 9_x, 4_x, d_x, 4_x, 9_x, 1_x)$
$(1_x, d_x, 4_x, 9_x, 4_x, d_x, d_x, 1_x, 9_x)$, $(1_x, d_x, 4_x, d_x, 1_x, 9_x, 4_x, 9_x, 1_x)$, $(1_x, d_x, 4_x, d_x, 1_x, 9_x, 9_x, 4_x, d_x)$
$(1_x, d_x, 9_x, 4_x, 9_x, d_x, 9_x, 4_x, 1_x)$, $(1_x, d_x, 9_x, 4_x, 9_x, d_x, d_x, 1_x, 4_x)$, $(1_x, d_x, 9_x, 9_x, 4_x, 1_x, 4_x, 9_x, d_x)$
$(1_x, d_x, 9_x, 9_x, 4_x, 1_x, d_x, 1_x, 4_x)$, $(1_x, d_x, 9_x, d_x, 1_x, 4_x, 4_x, 9_x, d_x)$, $(1_x, d_x, 9_x, d_x, 1_x, 4_x, 9_x, 4_x, 1_x)$
$(4_x, 1_x, 9_x, 1_x, 4_x, d_x, 9_x, d_x, 4_x)$, $(4_x, 1_x, 9_x, 1_x, 4_x, d_x, d_x, 9_x, 1_x)$, $(4_x, 1_x, 9_x, 9_x, d_x, 4_x, 1_x, 4_x, d_x)$
$(4_x, 1_x, 9_x, 9_x, d_x, 4_x, d_x, 9_x, 1_x)$, $(4_x, 1_x, 9_x, d_x, 9_x, 1_x, 1_x, 4_x, d_x)$, $(4_x, 1_x, 9_x, d_x, 9_x, 1_x, 9_x, d_x, 4_x)$
$(4_x, 1_x, d_x, 1_x, 4_x, 9_x, 9_x, d_x, 1_x)$, $(4_x, 1_x, d_x, 1_x, 4_x, 9_x, d_x, 9_x, 4_x)$, $(4_x, 1_x, d_x, 9_x, d_x, 1_x, 1_x, 4_x, 9_x)$
$(4_x, 1_x, d_x, 9_x, d_x, 1_x, d_x, 9_x, 4_x)$, $(4_x, 1_x, d_x, d_x, 9_x, 4_x, 1_x, 4_x, 9_x)$, $(4_x, 1_x, d_x, d_x, 9_x, 4_x, 9_x, d_x, 1_x)$
$(4_x, 9_x, 1_x, 1_x, d_x, 4_x, 9_x, 4_x, d_x)$, $(4_x, 9_x, 1_x, 1_x, d_x, 4_x, d_x, 1_x, 9_x)$, $(4_x, 9_x, 1_x, 9_x, 4_x, d_x, 1_x, d_x, 4_x)$
$(4_x, 9_x, 1_x, 9_x, 4_x, d_x, d_x, 1_x, 9_x)$, $(4_x, 9_x, 1_x, d_x, 1_x, 9_x, 1_x, d_x, 4_x)$, $(4_x, 9_x, 1_x, d_x, 1_x, 9_x, 9_x, 4_x, d_x)$
$(4_x, 9_x, d_x, 1_x, d_x, 9_x, 9_x, 4_x, 1_x)$, $(4_x, 9_x, d_x, 1_x, d_x, 9_x, d_x, 1_x, 4_x)$, $(4_x, 9_x, d_x, 9_x, 4_x, 1_x, 1_x, d_x, 9_x)$
$(4_x, 9_x, d_x, 9_x, 4_x, 1_x, d_x, 1_x, 4_x)$, $(4_x, 9_x, d_x, d_x, 1_x, 4_x, 1_x, d_x, 9_x)$, $(4_x, 9_x, d_x, d_x, 1_x, 4_x, 9_x, 4_x, 1_x)$
$(4_x, d_x, 1_x, 1_x, 9_x, 4_x, 9_x, 1_x, d_x)$, $(4_x, d_x, 1_x, 1_x, 9_x, 4_x, d_x, 4_x, 9_x)$, $(4_x, d_x, 1_x, 9_x, 1_x, d_x, 1_x, 9_x, 4_x)$
$(4_x, d_x, 1_x, 9_x, 1_x, d_x, d_x, 4_x, 9_x)$, $(4_x, d_x, 1_x, d_x, 4_x, 9_x, 1_x, 9_x, 4_x)$, $(4_x, d_x, 1_x, d_x, 4_x, 9_x, 9_x, 1_x, d_x)$
$(4_x, d_x, 9_x, 1_x, 9_x, d_x, 9_x, 1_x, 4_x)$, $(4_x, d_x, 9_x, 1_x, 9_x, d_x, d_x, 4_x, 1_x)$, $(4_x, d_x, 9_x, 9_x, 1_x, 4_x, 1_x, 9_x, d_x)$
$(4_x, d_x, 9_x, 9_x, 1_x, 4_x, d_x, 4_x, 1_x)$, $(4_x, d_x, 9_x, d_x, 4_x, 1_x, 1_x, 9_x, d_x)$, $(4_x, d_x, 9_x, d_x, 4_x, 1_x, 9_x, 1_x, 4_x)$
$(9_x, 1_x, 4_x, 1_x, 9_x, d_x, 4_x, d_x, 9_x)$, $(9_x, 1_x, 4_x, 1_x, 9_x, d_x, d_x, 4_x, 1_x)$, $(9_x, 1_x, 4_x, 4_x, d_x, 9_x, 1_x, 9_x, d_x)$
$(9_x, 1_x, 4_x, 4_x, d_x, 9_x, d_x, 4_x, 1_x)$, $(9_x, 1_x, 4_x, d_x, 4_x, 1_x, 1_x, 9_x, d_x)$, $(9_x, 1_x, 4_x, d_x, 4_x, 1_x, 4_x, d_x, 9_x)$

$(9_x, 1_x, d_x, 1_x, 9_x, 4_x, 4_x, d_x, 1_x)$, $(9_x, 1_x, d_x, 1_x, 9_x, 4_x, d_x, 4_x, 9_x)$, $(9_x, 1_x, d_x, 4_x, d_x, 1_x, 1_x, 9_x, 4_x)$
$(9_x, 1_x, d_x, 4_x, d_x, 1_x, d_x, 4_x, 9_x)$, $(9_x, 1_x, d_x, d_x, 4_x, 9_x, 1_x, 9_x, 4_x)$, $(9_x, 1_x, d_x, d_x, 4_x, 9_x, 4_x, d_x, 1_x)$
$(9_x, 4_x, 1_x, 1_x, d_x, 9_x, 4_x, 9_x, d_x)$, $(9_x, 4_x, 1_x, 1_x, d_x, 9_x, d_x, 1_x, 4_x)$, $(9_x, 4_x, 1_x, 4_x, 9_x, d_x, 1_x, d_x, 9_x)$
$(9_x, 4_x, 1_x, 4_x, 9_x, d_x, d_x, 1_x, 4_x)$, $(9_x, 4_x, 1_x, d_x, 1_x, 4_x, 1_x, d_x, 9_x)$, $(9_x, 4_x, 1_x, d_x, 1_x, 4_x, 4_x, 9_x, d_x)$
$(9_x, 4_x, d_x, 1_x, d_x, 4_x, 4_x, 9_x, 1_x)$, $(9_x, 4_x, d_x, 1_x, d_x, 4_x, d_x, 1_x, 9_x)$, $(9_x, 4_x, d_x, 4_x, 9_x, 1_x, 1_x, d_x, 4_x)$
$(9_x, 4_x, d_x, 4_x, 9_x, 1_x, d_x, 1_x, 9_x)$, $(9_x, 4_x, d_x, d_x, 1_x, 9_x, 1_x, d_x, 4_x)$, $(9_x, 4_x, d_x, d_x, 1_x, 9_x, 4_x, 9_x, 1_x)$
$(9_x, d_x, 1_x, 1_x, 4_x, 9_x, 4_x, 1_x, d_x)$, $(9_x, d_x, 1_x, 1_x, 4_x, 9_x, d_x, 9_x, 4_x)$, $(9_x, d_x, 1_x, 4_x, 1_x, d_x, 1_x, 4_x, 9_x)$
$(9_x, d_x, 1_x, 4_x, 1_x, d_x, d_x, 9_x, 4_x)$, $(9_x, d_x, 1_x, d_x, 9_x, 4_x, 1_x, 4_x, 9_x)$, $(9_x, d_x, 1_x, d_x, 9_x, 4_x, 4_x, 1_x, d_x)$
$(9_x, d_x, 4_x, 1_x, 4_x, d_x, 4_x, 1_x, 9_x)$, $(9_x, d_x, 4_x, 1_x, 4_x, d_x, d_x, 9_x, 1_x)$, $(9_x, d_x, 4_x, 4_x, 1_x, 9_x, 1_x, 4_x, d_x)$
$(9_x, d_x, 4_x, 4_x, 1_x, 9_x, d_x, 9_x, 1_x)$, $(9_x, d_x, 4_x, d_x, 9_x, 1_x, 1_x, 4_x, d_x)$, $(9_x, d_x, 4_x, d_x, 9_x, 1_x, 4_x, 1_x, 9_x)$
$(d_x, 1_x, 4_x, 1_x, d_x, 9_x, 4_x, 9_x, d_x)$, $(d_x, 1_x, 4_x, 1_x, d_x, 9_x, 9_x, 4_x, 1_x)$, $(d_x, 1_x, 4_x, 4_x, 9_x, d_x, 1_x, d_x, 9_x)$
$(d_x, 1_x, 4_x, 4_x, 9_x, d_x, 9_x, 4_x, 1_x)$, $(d_x, 1_x, 4_x, 9_x, 4_x, 1_x, 1_x, d_x, 9_x)$, $(d_x, 1_x, 4_x, 9_x, 4_x, 1_x, 4_x, 9_x, d_x)$
$(d_x, 1_x, 9_x, 1_x, d_x, 4_x, 4_x, 9_x, 1_x)$, $(d_x, 1_x, 9_x, 1_x, d_x, 4_x, 9_x, 4_x, d_x)$, $(d_x, 1_x, 9_x, 4_x, 9_x, 1_x, 1_x, d_x, 4_x)$
$(d_x, 1_x, 9_x, 4_x, 9_x, 1_x, 9_x, 4_x, d_x)$, $(d_x, 1_x, 9_x, 9_x, 4_x, d_x, 1_x, d_x, 4_x)$, $(d_x, 1_x, 9_x, 9_x, 4_x, d_x, 4_x, 9_x, 1_x)$
$(d_x, 4_x, 1_x, 1_x, 9_x, d_x, 4_x, d_x, 9_x)$, $(d_x, 4_x, 1_x, 1_x, 9_x, d_x, 9_x, 1_x, 4_x)$, $(d_x, 4_x, 1_x, 4_x, d_x, 9_x, 1_x, 9_x, d_x)$
$(d_x, 4_x, 1_x, 4_x, d_x, 9_x, 9_x, 1_x, 4_x)$, $(d_x, 4_x, 1_x, 9_x, 1_x, 4_x, 1_x, 9_x, d_x)$, $(d_x, 4_x, 1_x, 9_x, 1_x, 4_x, 4_x, d_x, 9_x)$
$(d_x, 4_x, 9_x, 1_x, 9_x, 4_x, 4_x, d_x, 1_x)$, $(d_x, 4_x, 9_x, 1_x, 9_x, 4_x, 9_x, 1_x, d_x)$, $(d_x, 4_x, 9_x, 4_x, d_x, 1_x, 1_x, 9_x, 4_x)$
$(d_x, 4_x, 9_x, 4_x, d_x, 1_x, 9_x, 1_x, d_x)$, $(d_x, 4_x, 9_x, 9_x, 1_x, d_x, 1_x, 9_x, 4_x)$, $(d_x, 4_x, 9_x, 9_x, 1_x, d_x, 4_x, d_x, 1_x)$
$(d_x, 9_x, 1_x, 1_x, 4_x, d_x, 4_x, 1_x, 9_x)$, $(d_x, 9_x, 1_x, 1_x, 4_x, d_x, 9_x, d_x, 4_x)$, $(d_x, 9_x, 1_x, 4_x, 1_x, 9_x, 1_x, 4_x, d_x)$
$(d_x, 9_x, 1_x, 4_x, 1_x, 9_x, 9_x, d_x, 4_x)$, $(d_x, 9_x, 1_x, 9_x, d_x, 4_x, 1_x, 4_x, d_x)$, $(d_x, 9_x, 1_x, 9_x, d_x, 4_x, 4_x, 1_x, 9_x)$
$(d_x, 9_x, 4_x, 1_x, 4_x, 9_x, 4_x, 1_x, d_x)$, $(d_x, 9_x, 4_x, 1_x, 4_x, 9_x, 9_x, d_x, 1_x)$, $(d_x, 9_x, 4_x, 4_x, 1_x, d_x, 1_x, 4_x, 9_x)$
$(d_x, 9_x, 4_x, 4_x, 1_x, d_x, 9_x, d_x, 1_x)$, $(d_x, 9_x, 4_x, 9_x, d_x, 1_x, 1_x, 4_x, 9_x)$, $(d_x, 9_x, 4_x, 9_x, d_x, 1_x, 4_x, 1_x, d_x)$