IACR Communications in Cryptology
ISSN 3006-5496, Vol. 2, No. 1, 32 pages.

https://doi.org/10.62056/a6ksdk5vt

Construction of Hadamard-based MixColumns Matrices Resistant to Related-Differential Cryptanalysis

Sonu Jha[1], Shun Li[2] and Danilo Gligoroski[1]

[1] Norwegian University of Science and Technology, Trondheim, Norway

[2] Chinese Academy of Sciences, Beijing, China

Abstract. In this paper, we study MDS matrices that are specifically designed to prevent the occurrence of related differentials. We investigate MDS matrices with a Hadamard structure and demonstrate that it is possible to construct 4×4 Hadamard matrices that effectively eliminate related differentials. Incorporating these matrices into the linear layer of AES-like block-ciphers/hash functions significantly mitigates the attacks that exploit the related differentials property. The central contribution of this paper is to identify crucial underlying relations that determine whether a given 4×4 Hadamard matrix exhibits related differentials. By satisfying these relations, the matrix ensures the presence of related differentials, whereas failing to meet them leads to the absence of such differentials. This offers effective mitigation of recently reported attacks on reduced-round AES. Furthermore, we propose a faster search technique to exhaustively verify the presence or absence of related differentials in Hadamard matrices over $\mathbb{F}_{2^n}^{8\times 8}$ which requires checking only a subset of involutory matrices in the set. Although most existing studies on constructing MDS matrices primarily focus on lightweight hardware/software implementations, our research additionally introduces a novel perspective by emphasizing the importance of MDS matrix construction in relation to their resistance against differential cryptanalysis.

Keywords: AES · Linear Layers · Hadamard Matrices · Related Differentials · Counter-measures · MDS-Matrix-Construction.

1 Introduction

The *Substitution-Permutation Network* (SPN) structure stands as one of the most widely accepted designs for block ciphers. In practice, permutation components are commonly implemented using linear operations. Their purpose is to spread internal dependencies as much as possible. Among these operations, maximum distance separable (MDS) matrices are highly favored as diffusion building blocks. Integrating MDS matrices as diffusion layers in iterative block ciphers allows us to achieve the desired number of differentially or linearly active nonlinear elements in a small number of rounds, resulting in designs with low latency.

Furthermore, designs that incorporate MDS matrices often benefit from straightforward and well-established security proofs, as demonstrated by the case of AES [DR02]. In fact, it is the elegant security proof provided by AES that has led to the widespread application of MDS matrices in the design of symmetric key primitives.

E-mail: sonu.k.jha@ntnu.no (Sonu Jha), lishun@ucas.ac.cn (Shun Li), danilog@ntnu.no (Danilo Gligoroski)

Received: 2025-01-13 Accepted: 2025-03-11

In [DR09], the authors presented a study on a class of linear transformations that are used in AES-like block ciphers. Their goal was to address the question of which properties of the linear transformation affect the probability of differentials and their characteristics over super-S-boxes. Based on that study, the authors introduced a property of linear transformations called *Related Differentials* which affects the probability values of differentials over a fixed key. They presented related differentials over the AES MixColumns transformation.

In [GBR22], using the related differentials caused by the current AES MixColumns transformation, they provided related differentials for up to four-round AES. And, their combinations with the zero-difference property introduced in [RBH17] resulted in new attacks up to 7-round AES. One way to avoid such attack extensions is to exploit MixColumns transformations without related differentials, which will be the main focus of this paper.

This brings to light the question of constructing MDS matrices which do not exhibit the property of related differentials, and therefore such attack extensions as [GBR22], which use the vulnerability of Mixcolumns transformations, could be avoided due to the absence of related differentials in the corresponding matrix used. In this paper, we answer this question by presenting feasible techniques towards the construction of such matrices.

Related work. When the implementation cost is the primary concern, there exist multiple approaches to search for a *lightweight* MDS matrix. Guo, Peyrin, and Poschmann introduced a method that involves finding a lightweight matrix, denoted as A, satisfying the property that raising A to the power of k results in an MDS matrix [GPP11, GPPR11]. This approach effectively reduces the implementation footprint and optimizes the chip area. The recursive constructions are further explored in [WWW13, Ber13, AF14, CLM16, GPV17, TTKS18, LSS+20].

Other endeavors aimed at discovering lightweight MDS matrices, in which the entire matrix is implemented, primarily focusing on selecting matrix entries with minimal hardware footprints [SKOP15, BKL16, LS16, LW16, SS16a, SS16b, LW17, SS17, JPST17, KLSW17, ZWS18, DL18, LSL+19]. This line of work involves constructing MDS matrices from specific classes of matrices, including circulant, involutory, Hadamard, and Toeplitz matrices.

In the constructions of the MDS matrices discussed above, the focus is on prioritizing efficiency rather than security. This is due to the assurance of cipher security provided by the wide-trail strategy and the MDS property. Until recently, [GBR22] provided a security analysis that takes advantage of related differentials originating from the MixColumn transformation of AES.

Our Contribution. In this paper, we use the notion of related differentials introduced in [DR09] to propose a new perspective on the construction of MDS matrices with respect to their resistance to related-differential cryptanalysis when used as a linear layer of a block cipher/hash function. The objective of this paper is to show that the resistance of a 4×4 MDS matrix M over $\mathbb{F}_{2^n}$ of a given structure to related differentials depends on certain equations that the matrix elements must not satisfy. Failing that, the matrix admits related differentials. The set of equations is deduced by analyzing a pair of related input differences, for which the corresponding pair of output differences is also related on the generalized map M. Whereas there are several matrix structures that are widely used in the designs of cryptographic primitives, in this paper, we aim to choose one with structural simplicity as the basis in order to show the construction of a resistant matrix. Since 4×4

circulant matrices by design always admit related differentials [1], we look into other classes of matrices which admit the *Maximum Distance Separable* (MDS) property. Matrices with Hadamard [BR00, SKOP15] and Toeplitz structures [SS16b] has been widely studied for their applications in cryptography, however, Toeplitz matrices have less structure and symmetry compared to Hadamard. Therefore, we use 4×4 MDS matrices with Hadamard structure as a pipeline to show the construction of a resistant matrix. For an in-depth exploration of generalized results concerning Hadamard MDS Matrices, one can refer to [PSA+18] and Section 2.3. Given Lemma 1 from [DR09] that proposes a bound on the weights of quartets satisfying the related differentials property, we propose Lemmas 2 and 3 which show how to choose minimal weights of generalized related input differences which are sufficient for deducing all the conditions in which the matrix admits related differentials. Note that the Lemmas 1, 2 and 3 are independent of the structure of the matrix, and can be utilized as a basis to derive similar conditions for different matrix structures. Using these valid input pairs with minimal weights, Theorem 3 shows that for the class of 4×4 MDS Hadamard matrices, there exist 28 equations which should be dissatisfied by the matrix to avoid the presence of related differentials. *Note that* the naive approach to find a 4×4 Hadamard MDS matrix without related differentials would be to confirm that no possible quartet of input and output difference pairs exist that satisfies this property, however, Theorem 3 reduces this complexity drastically to only 28 checks on matrix elements over $\mathbb{F}_{2^n}$ for any value of n. From the results derived in Theorem 3, we conclude using a faster experimental approach based on the equivalence class of matrices with respect to related differentials, that

- all MDS Hadamard matrices in the sets $\mathbb{F}_{2^3}^{4\times4}$ and $\mathbb{F}_{2^4}^{4\times4}$ have related differentials.
- in $\mathbb{F}_{2^n}^{4\times4}$ with $n > 4$, an exhaustive list of Hadamard MDS matrices devoid of related differentials can be generated in time $\mathcal{O}(2^{3n})$, which is 2^n times faster than brute-force.

We also present a list of some lightweight candidate matrices from the set of resistant matrices in $\mathbb{F}_{2^8}^{4\times4}$. We notice that to deterministically construct 8×8 Hadamard MDS matrices over $\mathbb{F}_{2^n}$ resistant to related differentials, one needs to have a complete characterization of the relations that the elements of the 8×8 matrix must not satisfy. Applying the methodology shown in Theorem 3 proves to be more cumbersome and complicated to characterize all the necessary and sufficient relations between the 8×8 matrix elements. Nevertheless, leveraging the results on equivalence classes of Hadamard matrices over $\mathbb{F}_{2^n}$ shown in [SKOP15], we propose Algorithm 3 to perform faster than exhaustive search for Hadamard MDS matrices in $\mathbb{F}_{2^n}^{8\times8}$ that are free of related differentials. This search technique is faster than an exhaustive search because we only need to check the subset of 8×8 involutory Hadamard matrices, which implies the same result for the entire matrix set as a consequence of Theorem 4. By performing experiments using this technique, we observed that all the Hadamard MDS matrices in sets $\mathbb{F}_{2^4}^{8\times8}$ and $\mathbb{F}_{2^5}^{8\times8}$ admit related differenitals. In summary, this paper brings to light the need and feasibility of research in the construction of differential cryptanalysis resistant MDS matrices of different dimensions and structures, in addition to the ongoing efforts in other strands of literature on MDS matrix construction, such as lightweight matrix constructions.

Outline. The paper is organized as follows. In Section 2 we present preliminaries on Hadamard Matrices, related differentials of linear layers [DR09], AES and attacks based on related differentials property. In Section 3 we present analytical proofs indicating the

[1] For a circulant matrix denoted as $\text{cir}(a, b, c, d)$, the related input pair of differences $([1, 0, \frac{c}{a}, 0], [0, \frac{d}{a}, 0, \frac{b}{a}])$ always result in related output difference pair after post-multiplication with the matrix for any value of $\{a, b, c, d\}$, thus forming related differentials (related difference and related differentials are defined in Definitions 1 and 2). [DR09] also discusses this fact in circulant matrices.

underlying relations the elements of the 4×4 Hadamard matrix must satisfy to form related differentials. Section 4 provides discussions on the construction of resistant MDS matrices by illustrating the implications of Theorem 3 over Hadamard MDS matrices in $\mathbb{F}_{2^3}^{4\times4}$, $\mathbb{F}_{2^4}^{4\times4}$ and $\mathbb{F}_{2^n}^{4\times4}$ with $n > 4$, and a faster than exhaustive experimental approach to generate all 4×4 resistant matrices over a given field. Additionally, we present discussions on the search for candidate lightweight matrices in the list of resistant matrices. In Section 5, we present an algorithm to perform faster than exhaustive search to find resistant matrices in $\mathbb{F}_{2^n}^{8\times8}$ by evaluating a representative subset of involutory matrices that generates the entire matrix set. We conclude the paper in Section 6. In appendix A, we show examples of matrices in $\mathbb{F}_{2^8}^{4\times4}$ with related differentials and the corresponding relations satisfied by their elements. Appendix B shows the lists of some resistant MDS Hadamard matrices in $\mathbb{F}_{2^8}^{4\times4}$, $\mathbb{F}_{2^6}^{4\times4}$ and $\mathbb{F}_{2^5}^{4\times4}$, followed by the list of a few candidate lightweight Hadamard MDS matrices in $\mathbb{F}_{2^8}^{4\times4}$ that are resistant to related differentials. We tabulate matrix spaces with no resistant matrices in Appendix C Table 15, and provide a brief guide on obtaining binary multiplication matrix of a field element in Appendix D.

2 Preliminaries

2.1 Operators and Notations

Let $\mathbb{F}_{2^n}$ denote a finite field of characteristic 2 and let $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$ denote its multiplicative cyclic group. Let a and b denote elements from the finite field $\mathbb{F}_{2^n}$. We use the terms $a + b$ and $a \oplus b$ in this paper which are equivalent and denote addition over finite fields of characteristic 2. The term $a \cdot b$ or simply ab denotes the multiplication in the field. The term $\frac{a}{b}$ denotes the operation $a \cdot b^{-1}$ in the field. $\hat{\mathbf{v}} = [v_0, v_1, \ldots, v_{m-1}]$ with $v_i \in \mathbb{F}_{2^n}$ denotes an m-element vector over the field. The function $\mathsf{wt}(\hat{\mathbf{v}})$ returns the total number of non-zero elements in $\hat{\mathbf{v}}$, often referred to as the *hamming weight* of $\hat{\mathbf{v}}$.

2.2 MDS Matrices

A square matrix M of order m over $\mathbb{F}_q$ is *MDS (Maximum Distance Separable)* if it satisfies the following equivalent properties:

- For any non-zero vector V, $\mathsf{wt}(V) + \mathsf{wt}(M \cdot V) \geq m + 1$.
- Every square submatrix of M is non-singular [MS77].

The first property ensures maximal diffusion, as even a single non-zero input affects all outputs.

Differential Branch Number The *differential branch number* of M, defined as

$$\mathcal{B}(M) = \min_{V \neq 0} \left(\mathsf{wt}(V) + \mathsf{wt}(M \cdot V) \right),$$

is $m + 1$ for MDS matrices. This guarantees optimal propagation of non-zero patterns in cryptographic primitives [DR02].

Cryptographic Relevance MDS matrices are critical in diffusion layers (e.g., AES's MixColumns). Their use ensures that minimal input changes propagate maximally, countering differential attacks. However, they often require computations over large fields, posing implementation trade-offs between security and efficiency.

2.3 Hadamard Matrices over $\mathbb{F}_{2^n}$

A Hadamard matrix is an $m \times m$ matrix whose entries are either $+1$ or -1, and whose rows (and columns) are mutually orthogonal (i.e., $HH^T = mI_m$). Such matrices have been widely studied due to their combinatorial properties and applications in signal processing, coding theory, and other areas.

In this work, however, we consider a different but related notion of Hadamard matrices over finite fields. Building upon the notation established in the paper [PSA+18], we wish to underscore the following property: in the case where the finite field over which Hadamard matrices are defined is $\mathbb{F}_{2^n}$, a Hadamard $m \times m$ MDS matrix is denoted as $M = \text{had}(a_0, a_1, \ldots, a_{m-1})$, comprising exactly m nonzero pairwise distinct elements. The $m \times m$ Hadamard matrix M formed by the elements $\{a_0, a_1, \ldots, a_{m-1}\}$ has entries $M[i, j] = a_{i \oplus j}$. Note that in a Hadamard MDS matrix, the m elements must be distinct from each other. This requirement stems from the fact that if two elements are equal, i.e., $a_i = a_j$, then a minor of order 2 with the value $a_i^2 + a_j^2 = 2a_i^2$ becomes zero in a finite field with characteristic 2.

The $m \times m$ matrix M denoted by $\text{had}(a_0, a_1, \ldots, a_{m-1})$ is depicted below:

$$M = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{m-2} & a_{m-1} \\ a_1 & a_0 & a_3 & \cdots & \ldots & \ldots \\ a_2 & a_3 & a_0 & \cdots & \ldots & \ldots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m-2} & \ldots & \ldots & \cdots & a_0 & \ldots \\ a_{m-1} & \ldots & \ldots & \cdots & \ldots & a_0 \end{pmatrix}.$$

From a differential cryptanalysis perspective, if the vector $\hat{\mathbf{b}} = [b_0, b_1, \ldots, b_{m-1}]$ denotes the input difference to the linear map M and the vector $\hat{\mathbf{c}} = [c_0, c_1, \ldots, c_{m-1}]$ denotes the the output difference, then we have $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}}$.

2.4 Related Differences and Related Differentials

In [DR09], authors defined the notion of Related Differences and Related Differentials. Let $\mathbb{F}_{2^n}$ be the underlying field over which the S-box of the block cipher is defined. Given the input difference vector $\hat{\mathbf{b}}$ and the MixColumns matrix M, let $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}}$ denote the corresponding output difference. The input/output difference pair $(\hat{\mathbf{b}}, \hat{\mathbf{c}})$ is called a differential. We restate below the definitions of *related differences* and *related differentials* from [DR09].

Definition 1. Two vectors $\hat{\mathbf{b}} = [b_0, b_1, \ldots, b_{m-1}]$ and $\hat{\mathbf{b}}' = [b'_0, b'_1, \ldots, b'_{m-1}]$ are related differences if and only if

$$b_i \cdot b'_i \cdot (b_i \oplus b'_i) = 0$$

$\forall i \in \{0, 1, 2, \ldots, m-1\}$.

Two related differences define a special type of second-order differential. Given a state $\hat{\boldsymbol{\alpha}} \in \mathbb{F}_{2^n}^m$, and the related differences $\hat{\mathbf{b}}$,$\hat{\mathbf{b}}'$, define a quartet of states as $(\hat{\boldsymbol{\alpha}},\ \hat{\boldsymbol{\alpha}} \oplus \hat{\mathbf{b}},\ \hat{\boldsymbol{\alpha}} \oplus \hat{\mathbf{b}}',\ \hat{\boldsymbol{\alpha}} \oplus \hat{\mathbf{b}} \oplus \hat{\mathbf{b}}')$. Note that this given quartet has a property that the sets $\{\alpha_i,\ \alpha_i \oplus b_i,\ \alpha_i \oplus b'_i,\ \alpha_i \oplus b_i \oplus b'_i\}$, for all i, contain only two distinct elements. This property is depicted in Figure 1.

$$\begin{tikzcd}
\alpha_i \arrow[r, leftrightarrow, "b_i \oplus b'_i"] \arrow[d, leftrightarrow, "b_i"'] \arrow[dr, leftrightarrow, "b'_i"] & \alpha_i \oplus b_i \oplus b'_i \arrow[d, leftrightarrow, "b_i"] \arrow[dl, leftrightarrow] \\
\alpha_i \oplus b_i \arrow[r, leftrightarrow, "b_i \oplus b'_i"'] & \alpha_i \oplus b'_i
\end{tikzcd}$$

Figure 1: Pictorial representation of Related Differences with associated quartet. If any one of b_i, b'_i, $b_i \oplus b'_i$ becomes zero, then the square collapses to a line.

Definition 2. Two differentials $(\hat{\mathbf{b}}, \hat{\mathbf{c}})$ and $(\hat{\mathbf{b}'}, \hat{\mathbf{c}'})$ are related differentials over a linear map M, if and only if $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}}$ and $\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'}$, where the differences $\hat{\mathbf{b}}, \hat{\mathbf{b}'}$ are related and the differences $\hat{\mathbf{c}}, \hat{\mathbf{c}'}$ are also related.

Observation: Consider two vectors $\hat{\mathbf{b}}$,$\hat{\mathbf{b}'}$ with all non-zero elements, i.e. $wt(\hat{\mathbf{b}}) = wt(\hat{\mathbf{b}'}) = m$. Now, if these two vectors are to be related differences, then according to Definition 1, it must be true that $b_i \oplus b'_i = 0$ for all i, since their elements are all non-zero. This can only happen if $\hat{\mathbf{b}} = \hat{\mathbf{b}'}$. Therefore, two distinct vectors with all non-zero elements cannot be related differences. We will use this observation in Section 3 in order to choose the necessary and sufficient weights for input/output differences that will be used in our analysis to prove Theorem 3. Note that cases involving trivial related differences, where one of the vectors $\hat{\mathbf{b}}$, $\hat{\mathbf{b}'}$, $\hat{\mathbf{b}} + \hat{\mathbf{b}'}$ is the zero vector, will be excluded from the discussion in later sections. This exclusion is due to the fact that such cases do not contribute to any meaningful attacks. We now restate below the following lemma from [DR09] which bounds the weight of the input/output difference pairs forming related differentials.

Lemma 1. *If $(\hat{\mathbf{b}}, \hat{\mathbf{c}})$ and $(\hat{\mathbf{b}'}, \hat{\mathbf{c}'})$ are related differentials over a linear map with an associated $m \times m$ multiplication matrix that is MDS, then*

$$\min\Big\{\mathsf{wt}(\hat{\mathbf{b}}) + \mathsf{wt}(\hat{\mathbf{c}}),\ \ \mathsf{wt}(\hat{\mathbf{b}'}) + \mathsf{wt}(\hat{\mathbf{c}'}),\ \ \mathsf{wt}(\hat{\mathbf{b}} \oplus \hat{\mathbf{b}'}) + \mathsf{wt}(\hat{\mathbf{c}} \oplus \hat{\mathbf{c}'})\Big\} \ \leq\ m + \Big\lfloor \frac{m}{3} \Big\rfloor.$$

Authors in [DR09] provide a combinatorial bound given as Lemma 1, to check the existence of related differentials over any given map with associated MDS matrix. According to this bound, if two differentials $(\hat{\mathbf{b}}, \hat{\mathbf{c}})$ and $(\hat{\mathbf{b}'}, \hat{\mathbf{c}'})$ are related, then the minimum of $[(\mathsf{wt}(\hat{\mathbf{b}}) + \mathsf{wt}(\hat{\mathbf{c}})), (\mathsf{wt}(\hat{\mathbf{b}'}) + \mathsf{wt}(\hat{\mathbf{c}'})), (\mathsf{wt}(\hat{\mathbf{b}''}) + \mathsf{wt}(\hat{\mathbf{c}''}))]$ should be at most $m + \lfloor \frac{m}{3} \rfloor$, where $\hat{\mathbf{b}''} = \hat{\mathbf{b}} \oplus \hat{\mathbf{b}'}$ and $\hat{\mathbf{c}''} = \hat{\mathbf{c}} \oplus \hat{\mathbf{c}'}$. This means that if one were to check whether a matrix M admits related differentials, it is sufficient to check all input/output difference pairs with combined weight of $m + \lfloor \frac{m}{3} \rfloor$ (which in case of $m = 4$ is 5) to reveal all the related differentials for the matrix.

The authors emphasize that matrices with special structures exist that has no related differentials in general. They show examples of matrices with Hadamard structures which allows no related differentials. The Hadamard MDS matrix denoted as $\mathrm{had}(1, 2, 4, 6)$ is used for linear transformation in the Anubis block cipher [BR00]. The authors show related differentials which exists for the given matrix. The related differentials it has are $([0, 0, 4, 6], [4, 0, 8, E])$ and $([8, E, 4, 0], [4, 6, 0, 0])$ and $([8, E, 0, 6], [0, 6, 8, E])$ where the pairs represent differential $(\hat{\mathbf{b}}, \hat{\mathbf{c}})$ in hexadecimal. However, if the matrix is replaced by $\mathrm{had}(1, 2, 4, 9)$, there are no related differentials. In Section 3, we focus on deducing conditions for 4 × 4 MDS Hadamard matrices using the related differentials property defined above which indicates if the matrix admits related differentials or not.

2.5 AES and Attack Preliminaries

Advanced Encryption Standard or AES [AES01, DR02] operates on a 4 × 4 array of bytes given as

$$\begin{bmatrix} \alpha_0 & \alpha_4 & \alpha_8 & \alpha_{12} \\ \alpha_1 & \alpha_5 & \alpha_9 & \alpha_{13} \\ \alpha_2 & \alpha_6 & \alpha_{10} & \alpha_{14} \\ \alpha_3 & \alpha_7 & \alpha_{11} & \alpha_{15} \end{bmatrix}$$

where elements are in column-major order. This array is referred to as the internal state of the cipher. The encryption algorithm consists of a certain number of transformation rounds where the internal state of the cipher is transformed utilizing 4 specific operations. The number of transformation rounds depends on the key size, and they are 10 rounds for a 128-bit key, 12 rounds for a 192-bit key and 14 rounds for a 256-bit key. The key operations of AES applied on the internal state in each round which are relevant for the discussion of this paper are reproduced below.

`AddRoundKey`: Round key bytes are combined with each byte of the state using bit-wise XOR.

`SubBytes`: Each byte of the state is replaced by another byte according to a lookup table through a non-linear substitution step.

`ShiftRow`: The i-th row is shifted left by i positions, where $i = 0, 1, 2, 3$.

`MixColumn`: Applies a linear transformation on each column of the state using a fixed MDS matrix.

`MixColumn` step is omitted in the last round and an additional `AddRoundKey` step is applied to produce the resulting ciphertext.

Two-round zero-difference property: In [RBH17], a relation was introduced over a 2-round SPN, called the zero-difference property. We restate Theorem 1 from [RBH17].

Theorem 1. *Let $\hat{\boldsymbol{\alpha}}, \hat{\boldsymbol{\beta}} \in \mathbb{F}_q^n$ and $\hat{\boldsymbol{\alpha}}^{'}, \hat{\boldsymbol{\beta}}^{'}$ constitute any pair of states generated from $\hat{\boldsymbol{\alpha}}, \hat{\boldsymbol{\beta}}$, satisfying the condition that for any $1 \leq i \leq n$, $(\alpha_i, \beta_i) = (\alpha_i^{'}, \beta_i^{'})$ or $(\alpha_i, \beta_i) = (\beta_i^{'}, \alpha_i^{'})$. Consequently, the difference $S \circ P \circ S(\alpha) \oplus S \circ P \circ S(\beta)$ and the difference $S \circ P \circ S(\alpha^{'}) \oplus S \circ P \circ S(\beta^{'})$ exhibit identical activity or (non-)zero occurrences in precisely the same components, where S, P are generic substitution and permutation layers of a SPN cipher.*

Recently, the authors of [GBR22] showed that, for Substitution-Permutation Networks, related differentials could be combined with two rounds of zero difference property. The Theorem 2 from [GBR22] is restated below.

Theorem 2. *Let $\hat{\boldsymbol{\alpha}} \in \mathbb{F}_q^n$ and $\hat{\boldsymbol{x}}, \hat{\boldsymbol{x}}' \in \mathbb{F}_q^n$ be two related differences, then the differences $F(\hat{\boldsymbol{\alpha}}) \oplus F(\hat{\boldsymbol{\alpha}} \oplus \hat{\boldsymbol{x}})$ and $F(\hat{\boldsymbol{\alpha}} \oplus \hat{\boldsymbol{x}}') \oplus F(\hat{\boldsymbol{\alpha}} \oplus \hat{\boldsymbol{x}} \oplus \hat{\boldsymbol{x}}')$ exhibit zero-difference pattern where $F = P \circ S \circ P \circ S$.*

This combination allows to extend the zero-difference property to more than two rounds of SPNs. In the case of AES, the MixColumn matrix $cir(2, 3, 1, 1)$ contains the following sets of related differentials (see [DR09, p. 66]) which is used in [GBR22] to mount the key-recovery attack up to 7 rounds.

$\hat{\mathbf{b}}$	$\hat{\mathbf{c}}$	$\hat{\mathbf{b}'}$	$\hat{\mathbf{c}'}$	$\hat{\mathbf{b}}+\hat{\mathbf{b}'}$	$\hat{\mathbf{c}}+\hat{\mathbf{c}'}$
$[0,1,4,7]$	$[0,9,0,\ \mathrm{B}]$	$[5,1,0,7]$	$[\mathrm{E},0,\mathrm{D},0]$	$[5,0,4,0]$	$[\mathrm{E},9,\mathrm{D},\mathrm{B}]$
$[0,1,0,3]$	$[0,1,4,7]$	$[2,0,1,0]$	$[5,1,0,7]$	$[2,1,1,3]$	$[5,0,4,0]$
$[7,0,7,7]$	$[9,\mathrm{E},0,0]$	$[7,7,7,0]$	$[0,0,9,\mathrm{E}]$	$[0,7,0,7]$	$[9,\mathrm{E},9,\mathrm{E}]$
$[0,3,2,0]$	$[7,0,7,1]$	$[2,0,0,3]$	$[7,1,7,0]$	$[2,3,2,3]$	$[0,1,0,1]$

It is evident that the attacks discussed above requires the presence of related differentials in the underlying MixColumns matrix. Section 3 focuses on the construction of MDS matrices devoid of related differentials that makes the attack extension discussed above ineffective.

3 Analyzing Related Differential Properties over 4×4 Hadamard Matrices

We aim for a generalized analysis of 4 × 4 Hadamard matrices by looking for vectors $\hat{\mathbf{b}}$, $\hat{\mathbf{c}}$, $\hat{\mathbf{b}'}$, $\hat{\mathbf{c}'}$ which form related differentials. We begin the analysis by stating Lemmas 2 and 3 which utilizes the MDS property to determine all the valid pairs of related input differences with minimum weights which can be used in our analysis to derive the conditions under which the map admits related differentials. In Theorem 3, we use these generalised valid pairs of related input differences to compute the conditions under which the output differences also turns out to be related.

Lemma 2. *If* $(\hat{\mathbf{b}}, \hat{\mathbf{b}'})$ *are related differences containing* m *elements each, then differences* $(\hat{\mathbf{b}}, \hat{\mathbf{b}''} = \hat{\mathbf{b}} \oplus \hat{\mathbf{b}'})$ *and* $(\hat{\mathbf{b}'}, \hat{\mathbf{b}''})$ *are related differences with*

$$\mathsf{wt}(\hat{\mathbf{b}}) + \mathsf{wt}(\hat{\mathbf{b}'}) + \mathsf{wt}(\hat{\mathbf{b}''}) \leq 2m$$

Proof. According to Definition 1, we know that

$$b_i \cdot b'_i(b_i \oplus b'_i) = 0,\ \ i = 0, \dots, m-1$$

then, the differences $(\hat{\mathbf{b}}, \hat{\mathbf{b}''})$ are related differences since we have

$$b_i \cdot b''_i(b_i \oplus b''_i) = b_i \cdot (b_i \oplus b'_i)(b_i \oplus b_i \oplus b'_i) = 0$$

and similarly, the differences $(\hat{\mathbf{b}'}, \hat{\mathbf{b}''})$ are related differences since we have

$$b'_i \cdot b''_i(b'_i \oplus b''_i) = b'_i \cdot (b_i \oplus b'_i)(b'_i \oplus b_i \oplus b'_i) = 0$$

If $(\hat{\mathbf{b}}, \hat{\mathbf{b}'})$ are related, this implies that either $b_i = 0$ or $b'_i = 0$ or $b_i \oplus b'_i = b''_i = 0$. This means that for every $0 \leq i < m$ one of $b_i,\ b'_i,\ b''_i$ should be zero. Therefore the sum of weights of these vectors can be at most $3m - m = 2m$. □

In our analysis, we consider the case when $m = 4$. From Lemma 2, we know that $\mathsf{wt}(\hat{\mathbf{b}}) + \mathsf{wt}(\hat{\mathbf{b}'}) + \mathsf{wt}(\hat{\mathbf{b}''}) \leq 2 \cdot 4 = 8$ and similarly $\mathsf{wt}(\hat{\mathbf{c}}) + \mathsf{wt}(\hat{\mathbf{c}'}) + \mathsf{wt}(\hat{\mathbf{c}''}) \leq 2 \cdot 4 = 8$. So in order to check whether a matrix admits related differentials, we can begin our analysis with two input differences among $\hat{\mathbf{b}}$, $\hat{\mathbf{b}'}$ and $\hat{\mathbf{b}''}$ which have minimum weights.

The idea is to investigate under what conditions a given matrix admits related differentials when the two of the input differences have minimum weights. It is straightforward to see that the minimum weights a pair of input related differences can have are $(1,1)$, $(1,2)$, $(1,3)$, $(1,4)$, $(2,2)$, or $(2,3)$.

Lemma 3. *If $\hat{\mathbf{b}}$, $\hat{\mathbf{b}'}$ are related differences and an input pair to a 4×4 MDS linear map M where $(\mathsf{wt}(\hat{\mathbf{b}}), \mathsf{wt}(\hat{\mathbf{b}'})) = (1, 1)$ or $(\mathsf{wt}(\hat{\mathbf{b}}), \mathsf{wt}(\hat{\mathbf{b}'})) = (1, 2)$, then $(\hat{\mathbf{b}}, \hat{\mathbf{c}})$ and $(\hat{\mathbf{b}'}, \hat{\mathbf{c}'})$ can never form related differentials, where $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}}$ and $\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'}$.*

Proof. Due to the MDS property, the input difference $\hat{\mathbf{b}}$ having weight 1 will always result in the output difference $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}}$ which has weight 4. So for the case when $(\mathsf{wt}(\hat{\mathbf{b}}), \mathsf{wt}(\hat{\mathbf{b}'})) = (1, 1)$, we will have $(\mathsf{wt}(\hat{\mathbf{c}}), \mathsf{wt}(\hat{\mathbf{c}'})) = (4, 4)$. Therefore, according to the observation presented in Section 2.4, it implies that $\hat{\mathbf{c}} = \hat{\mathbf{c}'}$.

When $(\mathsf{wt}(\hat{\mathbf{b}}), \mathsf{wt}(\hat{\mathbf{b}'})) = (1, 2)$, then $(\mathsf{wt}(\hat{\mathbf{c}}), \mathsf{wt}(\hat{\mathbf{c}'}))$ can either be $(4, 3)$ or $(4, 4)$. We already know that two distinct differences with weights $(4, 4)$ cannot be related. Therefore when $(\mathsf{wt}(\hat{\mathbf{c}}), \mathsf{wt}(\hat{\mathbf{c}'})) = (4, 3)$, we must have $\mathsf{wt}(\hat{\mathbf{c}''} = \hat{\mathbf{c}} + \hat{\mathbf{c}'}) = 8 - 4 - 3 = 1$. As $\hat{\mathbf{b}}$, $\hat{\mathbf{b}'}$ are related differences, $\mathsf{wt}(\hat{\mathbf{b}''} = \hat{\mathbf{b}} + \hat{\mathbf{b}'})$ can be equal to either 1 or 3. Since $\mathsf{wt}(\hat{\mathbf{c}''}) = 1$, we must have $\mathsf{wt}(\hat{\mathbf{b}''}) = 4$ from the MDS property, and hence the input differences with weights $(1, 2)$ cannot form related output differences. □

Valid Weights: Omitting the invalid weights shown in Lemma 3, we see that input difference pairs with weights $(1, 3)$, $(1, 4)$, $(2, 2)$, and $(2, 3)$ can form related differentials and hence we consider input differences with these weight combinations for our analysis. Moreover in our analysis, we only consider input differentials with weights $(1, 4)$, $(2, 2)$, and $(2, 3)$. We omit the case of $(\mathsf{wt}(\hat{\mathbf{b}}), \mathsf{wt}(\hat{\mathbf{b}'})) = (1, 3)$ because $\mathsf{wt}(\hat{\mathbf{b}''} = \hat{\mathbf{b}} + \hat{\mathbf{b}'})$ in this case can either be 2 or 4. Since we already consider the case of input pairs with weights $(1, 4)$ in our analysis, so the case with weights $(1, 3)$ implies the same analytical result as $(1, 4)$.

Theorem 3. *Let us denote as $\{a, b, c, d\}$ the 4-element subset of $\mathbb{F}_{2^n}$ and let M denote a 4×4 MDS matrix with Hadamard structure formed by the elements $\{a, b, c, d\}$ as,*

$$M = \begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}$$

The matrix M is devoid of related differentials, if and only if the elements in M do not solve any equation from the following list of 28 equations denoted as $\mathbf{R}$:

$$ab + cd = \begin{cases} a^2 + c^2 \\ a^2 + d^2 \\ b^2 + c^2 \\ b^2 + d^2 \end{cases} \quad ac + bd = \begin{cases} a^2 + b^2 \\ a^2 + d^2 \\ b^2 + c^2 \\ c^2 + d^2 \end{cases} \quad ad + bc = \begin{cases} a^2 + b^2 \\ a^2 + c^2 \\ b^2 + d^2 \\ c^2 + d^2 \end{cases}$$

We note that the same property follows for the inverse map M^{-1} where

$$M^{-1} = \begin{bmatrix} a^\star & b^\star & c^\star & d^\star \\ b^\star & a^\star & d^\star & c^\star \\ c^\star & d^\star & a^\star & b^\star \\ d^\star & c^\star & b^\star & a^\star \end{bmatrix}$$

Proof. We firstly prove the statement on M^{-1}. If M could lead to the 28 relations about coefficients (a, b, c, d) from M, then M^{-1} could lead to the 28 relations about its coefficients

$$a(a{+}b{+}c{+}d) = \begin{cases} a^2+b^2 \\ a^2+c^2 \\ a^2+d^2 \end{cases} b(a{+}b{+}c{+}d) = \begin{cases} b^2+a^2 \\ b^2+c^2 \\ b^2+d^2 \end{cases} c(a{+}b{+}c{+}d) = \begin{cases} c^2+a^2 \\ c^2+b^2 \\ c^2+d^2 \end{cases}$$

$$d(a{+}b{+}c{+}d) = \begin{cases} d^2+a^2 \\ d^2+b^2 \\ d^2+c^2 \end{cases} a+b+c+d = \begin{cases} a \\ b \\ c \\ d \end{cases}$$

$(a^\star, b^\star, c^\star, d^\star)$ and these 28 relations exactly correspond to the original relations of (a, b, c, d). Actually we could deduce that

$$\begin{cases} a^\star = \frac{a(a+b+c+d)^2}{det(M)} \\ b^\star = \frac{b(a+b+c+d)^2}{det(M)} \\ c^\star = \frac{c(a+b+c+d)^2}{det(M)} \\ d^\star = \frac{d(a+b+c+d)^2}{det(M)} \end{cases}$$

Then substituting these value into the original 28 relations, as the degrees of left and right side of each relation are same, we could divide the same value such as $\frac{(a+b+c+d)^2}{det(M)}$ or $\frac{(a+b+c+d)^4}{det(M)^2}$.

The proof proceeds by analyzing multiple cases and sub-cases, each corresponding to different weight distributions of the related input vectors $\hat{\mathbf{b}}$ and $\hat{\mathbf{b}}'$. These weight distributions are chosen based on the conditions established in Lemmas 2 and 3, ensuring that only the relevant cases are considered.

For each case, we begin by selecting input vectors $\hat{\mathbf{b}}$ and $\hat{\mathbf{b}}'$, which may contain both fixed constants and unknown elements over the field. We then compute the corresponding output differences, $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}}$ and $\hat{\mathbf{c}}' = M \cdot \hat{\mathbf{b}}'$, and solve for the unknowns under the condition that $(\hat{\mathbf{c}}, \hat{\mathbf{c}}')$ remains a related differential pair. By systematically iterating through all valid cases and sub-cases, we derive a set of 28 necessary and sufficient equations that determine whether M admits related differentials.

If any of these equations hold, M permits related differentials; otherwise, it does not. Additionally, some cases lead to contradictions with the MDS property, making them impossible. In such case, we explicitly highlight these contradictions, while omitting redundant derivations. We now begin with the first case.

3.1 Analysis When $\mathsf{wt}(\hat{\mathbf{b}}) = 2$ and $\mathsf{wt}(\hat{\mathbf{b}}') = 2$

The related input difference pairs with weight 2 each are given as:

1. $\hat{\mathbf{b}} = [w, 0, 0, x]$ and $\hat{\mathbf{b}}'$ equals $[0, y, z, 0]$, which simplifies to $\hat{\mathbf{b}} = [1, 0, 0, x']$ and $\hat{\mathbf{b}}' = [0, y', z', 0]$. Here, x, y, z are divided by w without affecting the related differential properties.

2. $\hat{\mathbf{b}} = [w, 0, x, 0]$ and $\hat{\mathbf{b}}'$ equals $[0, y, 0, z]$, simplifying to $\hat{\mathbf{b}} = [1, 0, x', 0]$ and $\hat{\mathbf{b}}' = [0, y', 0, z']$.

3. $\hat{\mathbf{b}} = [x, w, 0, 0]$ and $\hat{\mathbf{b}}'$ equals $[0, 0, y, z]$, simplifying to $\hat{\mathbf{b}} = [x', 1, 0, 0]$ and $\hat{\mathbf{b}}' = [0, 0, y', z']$.

4. $\hat{\mathbf{b}} = [x, y, 0, 0]$ and $\hat{\mathbf{b}'}$ equals either $[x, 0, z, 0]$ or $[x, 0, 0, z]$, simplifying to $\hat{\mathbf{b}} = [1, y', 0, 0]$ and $\hat{\mathbf{b}'} = [1, 0, z', 0]$ or $[1, 0, 0, z']$.
5. $\hat{\mathbf{b}} = [x, 0, y, 0]$ and $\hat{\mathbf{b}'}$ equals $[x, 0, 0, z]$, simplifying to $\hat{\mathbf{b}} = [1, 0, y', 0]$ and $\hat{\mathbf{b}'} = [1, 0, 0, z']$.

where $x, y, z, w \in \mathbb{F}_{2^n}$ are unknowns. The following subsections analyze the solutions.

3.1.1 Case 1: $\hat{\mathbf{b}} = [1, 0, 0, x]$ and $\hat{\mathbf{b}'} = [0, y, z, 0]$

For this case, the output differences are given by:

$$\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}} = [a + dx, b + cx, c + bx, d + ax]$$

$$\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'} = [by + cz, ay + dz, dy + az, cy + bz]$$

Since both $\hat{\mathbf{c}}, \hat{\mathbf{c}'}$ have at least 3 non-zero elements and cannot have 4 simultaneously, at least two of the indices must be equal and nonzero. Assume that is $\mathbf{c_0} = \mathbf{c'_0}, \mathbf{c_1} = \mathbf{c'_1}$

$$\begin{cases} a + dx = by + cz \neq 0 \\ b + cx = ay + dz \neq 0 \end{cases} \tag{1}$$

Here we have another 2 cases:

Subcase 1.1: One Zero Element in $\hat{\mathbf{c}}$

$\hat{\mathbf{c}}$ has one zero, assume it is $\mathbf{c_2} = c + bx$. Then $x = \frac{c}{b}$, equation 1 turns to be

$$\begin{cases} a + \frac{dc}{b} = by + cz \\ b + \frac{c^2}{b} = ay + dz \end{cases},$$

it can be deduced that

$$y = \frac{c^3 + c(b^2 + d^2) + abd}{b(ac + bd)},$$

$$z = \frac{b^3 + b(a^2 + c^2) + acd}{b(ac + bd)}.$$

Furthermore, $\mathbf{c'_3} = cy + bz = 0$ or is equal to $\mathbf{c_3} = d + ax$. Substitute the value of y, z into $\mathbf{c'_3}$ leads to

$$\frac{(b^2 + c^2 + ab + cd)^2}{b(ac + bd)},$$

if $\mathbf{c_3}' = 0$ then,

$$ab + cd = b^2 + c^2 \tag{2}$$

or if $\mathbf{c'_3} = \mathbf{c_3}$ then,

$$\frac{ac + bd}{b} = \frac{(b^2 + c^2 + ab + cd)^2}{b(ac + bd)}, \tag{3}$$

equation 3 can be transformed into $(b + c)(a + b + c + d) = 0$, which contradicts the MDS condition.

Along the similar lines of the analysis shown above, if we take $\mathbf{c_1} = 0$, then we have $x = \frac{b}{c}$. Solving for the variables y, z by equating $\mathbf{c'_2} = \mathbf{c_2}$,$\mathbf{c'_3} = \mathbf{c_3}$ and substituting the values in the equation $\mathbf{c'_0} = 0$ gives equation 2. Similar impossibility result follow when we have $\mathbf{c'_0} = \mathbf{c_0}$.

Similarly if we take $\mathbf{c_0} = 0$, then $x = \frac{a}{d}$. Assume $\mathbf{c_2} = \mathbf{c'_2}, \mathbf{c_3} = \mathbf{c'_3}$, then we have the following solutions for the remaining unknowns

$$y = \frac{a^3 + ab^2 + ad^2 + bcd}{acd + bd^2}$$
$$z = \frac{d^3 + a^2d + c^2d + abc}{acd + bd^2}$$

Substituting these values in $\mathbf{c_1'}$ gives

$$\frac{\left(a^2 + ab + cd + d^2\right)^2}{acd + bd^2}$$

Then if $\mathbf{c_1'} = 0$, we have

$$a^2 + d^2 = ab + cd \tag{4}$$

otherwise if $\mathbf{c_1'} = \mathbf{c_1}$, we have the impossible relation $(a + d)(a + b + c + d) = 0$. When we have $\mathbf{c_3} = 0 \implies x = \frac{d}{a}$, then by solving for y, z in equations $\mathbf{c_0'} = \mathbf{c_0}$, $\mathbf{c_1'} = \mathbf{c_1}$ and substituting in $\mathbf{c_2'} = 0$ and $\mathbf{c_2'} = \mathbf{c_2}$, we respectively get equation 4 and a similar impossible case.

If we swap y, z in $\hat{\mathbf{b}}'$, we have

$$\hat{\mathbf{c}'} = [bz + cy, az + dy, dz + ay, cz + by]$$

Then for $\mathbf{c_0} = 0 \implies x = \frac{a}{d}$, solving unknowns in $\mathbf{c_1'} = \mathbf{c_1}$, $\mathbf{c_3'} = \mathbf{c_3}$ and substituting in $\mathbf{c_2'} = dz + ay = 0$ gives

$$ac + bd = a^2 + d^2 \tag{5}$$

Impossibility results follow for substituting values of y, z in $\mathbf{c_2'} = \mathbf{c_2}$.

For $\mathbf{c_3} = 0 \implies x = \frac{d}{a}$, solving unknowns in equations $\mathbf{c_0'} = \mathbf{c_0}$, $\mathbf{c_2'} = \mathbf{c_2}$ and substituting the values in: $\mathbf{c_1'} = az + dy = 0$ gives equation 5, and $\mathbf{c_1'} = \mathbf{c_1}$ indicates a contradiction with the MDS property.

Following the similar methodology, for both instances $\mathbf{c_1} = 0 \implies x = \frac{b}{c}$ and $\mathbf{c_2} = 0 \implies x = \frac{c}{b}$, we get the relation

$$ac + bd = c^2 + b^2 \tag{6}$$

Subcase 1.2: No Zero Elements in $\hat{\mathbf{c}}$

If $\hat{\mathbf{c}}$ has no zero elements, then there must be a zero element from $\hat{\mathbf{c}'}$, otherwise, if both $\hat{\mathbf{c}}, \hat{\mathbf{c}'}$ are full non-zero, they must be completely equal, which means $M \cdot (\hat{\mathbf{b}} + \hat{\mathbf{b}'}) = 0$ or $M \cdot [1, y, z, x] = 0$, which is impossible. So we assume $dy + az = 0$ and $cy + bz = d + ax \neq 0$, solve the equation system with 4 equations and 3 variables:

$$\begin{cases} a + dx = by + cz \\ b + cx = ay + dz \\ 0 = dy + az \\ d + ax = cy + bz \end{cases} \tag{7}$$

which leads to $a^2 + d^2 + ab + cd = ac + bd$ which can be simplified to $(a+d)(a+b+c+d) = 0$, which is also impossible.

3.1.2 Case 2: $\hat{\mathbf{b}} = [1, 0, x, 0]$ and $\hat{\mathbf{b}'} = [0, y, 0, z]$

We have $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}} = [a + cx, b + dx, c + ax, d + bx]$ and $\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'} = [by + dz, ay + cz, dy + bz, cy + az]$. If we swap c and d, and exchange the third and fourth elements of $\hat{\mathbf{c}}, \hat{\mathbf{c}'}$, then it results in Case 1 again. Therefore, we omit a step by step description and provide table 1 indicating iterative deductions of each relation falling under this case of input pairs. Note that if we swap y, z in $\hat{\mathbf{b}}$, then following the similar iterations as in table 1 we get two similar relations where L.H.S is $ad + bc$.

Table 1: Relations for $\hat{\mathbf{b}} = [1, 0, x, 0]$ and $\hat{\mathbf{b}'} = [0, y, 0, z]$

Iterations	Steps	Results
$\mathbf{c_0} = 0 \implies x = \frac{a}{c}$	Solve unknowns in: $\mathbf{c_2} = \mathbf{c'_2}, \mathbf{c_3} = \mathbf{c'_3}$ Substitute in: $\mathbf{c'_1} = 0$	$ab + cd = a^2 + c^2$
$\mathbf{c_2} = 0 \implies x = \frac{c}{a}$	Solve unknowns in: $\mathbf{c_0} = \mathbf{c'_0}, \mathbf{c_1} = \mathbf{c'_1}$ Substitute in: $\mathbf{c'_3} = 0$	$ab + cd = a^2 + c^2$
$\mathbf{c_1} = 0 \implies x = \frac{b}{d}$	Solve unknowns in: $\mathbf{c_2} = \mathbf{c'_2}, \mathbf{c_3} = \mathbf{c'_3}$ Substitute in: $\mathbf{c'_0} = 0$	$ab + cd = b^2 + d^2$
$\mathbf{c_3} = 0 \implies x = \frac{d}{b}$	Solve unknowns in: $\mathbf{c_0} = \mathbf{c'_0}, \mathbf{c_1} = \mathbf{c'_1}$ Substitute in: $\mathbf{c'_3} = 0$	$ab + cd = b^2 + d^2$

3.1.3 Case 3: $\hat{\mathbf{b}} = [x, 1, 0, 0]$ and $\hat{\mathbf{b}'} = [0, 0, y, z]$

We have $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}} = [b + ax, a + bx, d + cx, c + dx]$ and $\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'} = [cy + dz, dy + cz, ay + bz, by + az]$. If we swap b and d, and permute the elements of $\hat{\mathbf{c}}, \hat{\mathbf{c}'}$ by $(1, 4, 3, 2)$, then it results in Case 1 again. The relations are discussed in table 2. If we swap y, z in $\hat{\mathbf{b}'}$, then following the similar iterations we get two similar relations where L.H.S is $ad + bc$.

Table 2: Relations for $\hat{\mathbf{b}} = [x, 1, 0, 0]$ and $\hat{\mathbf{b}'} = [0, 0, y, z]$

Iterations	Steps	Results
$\mathbf{c_0} = 0 \implies x = \frac{b}{a}$	Solve unknowns in: $\mathbf{c_1} = \mathbf{c'_1}, \mathbf{c_3} = \mathbf{c'_3}$ Substitute in: $\mathbf{c'_2} = 0$	$ac + bd = a^2 + b^2$
$\mathbf{c_1} = 0 \implies x = \frac{a}{b}$	Solve unknowns in: $\mathbf{c_0} = \mathbf{c'_0}, \mathbf{c_2} = \mathbf{c'_2}$ Substitute in: $\mathbf{c'_3} = 0$	$ac + bd = a^2 + b^2$
$\mathbf{c_2} = 0 \implies x = \frac{d}{c}$	Solve unknowns in: $\mathbf{c_1} = \mathbf{c'_1}, \mathbf{c_3} = \mathbf{c'_3}$ Substitute in: $\mathbf{c'_0} = 0$	$ac + bd = c^2 + d^2$
$\mathbf{c_3} = 0 \implies x = \frac{c}{d}$	Solve unknowns in: $\mathbf{c_0} = \mathbf{c'_0}, \mathbf{c_2} = \mathbf{c'_2}$ Substitute in: $\mathbf{c'_1} = 0$	$ac + bd = c^2 + d^2$

3.1.4 Case 4: $\hat{\mathbf{b}} = [1, y, 0, 0]$ and $\hat{\mathbf{b}'} = [1, 0, z, 0]$

We have $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}} = [a + by, b + ay, c + dy, d + cy]$ and $\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'} = [a + cz, b + dz, c + az, d + bz]$. Since $\hat{\mathbf{c}}$ and $\hat{\mathbf{c}'}$ have at most 1 zero elements, then at least two of the elements from them are equal. Assume $y = \frac{c}{b}z = \frac{d}{a}z$, then $ac + bd = 0$, which contradicts the MDS property. Similar argument follows for the case $\hat{\mathbf{b}'} = [1, 0, 0, z]$.

3.1.5 Case 5: $\hat{\mathbf{b}} = [1, 0, y, 0]$ and $\hat{\mathbf{b}'} = [1, 0, 0, z]$

We have $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}} = [a+cy, b+dy, c+ay, d+by]$ and $\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'} = [a+dz, b+cz, c+bz, d+az]$. Then it can be lead to contradiction similarly as Case 4.

Therefore, M admits related differentials where $(\mathsf{wt}(\hat{\mathbf{b}}), \mathsf{wt}(\hat{\mathbf{b}'})) = (2, 2)$, if and only if the elements of M satisfy at least one of the 12 relations deduced.

3.2 Analysis When $\mathsf{wt}(\hat{\mathbf{b}}) = 2$ and $\mathsf{wt}(\hat{\mathbf{b}'}) = 3$

In this section, we analyze input difference pairs having weights 2 and 3. Since the pair has only one non-zero element in the same index, we can move this non-zero element to the first index. A list of these input difference pairs are given below.

1. $\hat{\mathbf{b}} = [w, x, 0, 0]$ and $\hat{\mathbf{b}'} = [w, 0, y, z]$, which can be simplified to $\hat{\mathbf{b}} = [1, x', 0, 0]$ and $\hat{\mathbf{b}'} = [1, 0, y', z']$.
2. $\hat{\mathbf{b}} = [w, 0, x, 0]$ and $\hat{\mathbf{b}'} = [w, y, 0, z]$, which can be simplified to $\hat{\mathbf{b}} = [1, 0, x', 0]$ and $\hat{\mathbf{b}'} = [1, y', 0, z']$.
3. $\hat{\mathbf{b}} = [w, 0, 0, x]$ and $\hat{\mathbf{b}'} = [w, y, z, 0]$, which can be simplified to $\hat{\mathbf{b}} = [1, 0, 0, x']$ and $\hat{\mathbf{b}'} = [1, y', z', 0]$.

where x, y, z, w are unknowns elements from $\mathbb{F}_{2^n}$.

3.2.1 Case 1: $\hat{\mathbf{b}} = [1, x, 0, 0]$ and $\hat{\mathbf{b}'} = [1, 0, y, z]$

We have $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}} = [a + bx, b + ax, c + dx, d + cx]$ and $\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'} = [a + cy + dz, b + dy + cz, c + ay + bz, d + by + az]$. Since $\hat{\mathbf{c}}$ has at most 1 zero, we have another 2 cases:

Subcase 1.1: $\hat{\mathbf{c}}$ has one zero

Assume it is $\mathbf{c_0} = a + bx \implies x = \frac{a}{b}$. $b + ax \neq 0, c + dx \neq 0$, and $d + cx \neq 0$. Because the corresponding elements from $\hat{\mathbf{c}'}$ cannot be full zeros due to MDS property, we have at least one equation assuming it is $\mathbf{c_1} = \mathbf{c'_1}$, or $b + ax = b + dy + cz \neq 0$. If $c + ay + bz = 0$, then we have equations

$$\begin{cases} \frac{a^2}{b} = dy + cz \\ c = ay + bz \end{cases} \tag{8}$$

which leads to the solution of

$$\begin{cases} y = \frac{a^2+c^2}{ac+bd} \\ z = \frac{a^3+bcd}{b(ac+bd)} \end{cases}$$

substitute the value of x, y, z into the last elements of $\hat{\mathbf{c}}, \hat{\mathbf{c}'}$, either

$$d + by + az = 0$$

which leads to $a^2 + ab + bc + bd = 0$, which can be expressed as

$$b(a + b + c + d) = a^2 + b^2$$

or

$$d + by + az = d + cx$$

which leads to $a^2 + ab + ac + bc = 0$, which is impossible.

If $c + ay + bz \neq 0$, then we have equations

$$\begin{cases} \frac{a^2}{b} = dy + cz \\ \frac{ad}{b} = ay + bz \end{cases} \tag{9}$$

which leads to the solution of

$$\begin{cases} y = \frac{a(ab+cd)}{b(ac+bd)} \\ z = \frac{a(a^2+d^2)}{b(ac+bd)} \end{cases}$$

substituting the value of x, y, z into the last elements of $\hat{\mathbf{c}}, \hat{\mathbf{c}'}$, gives either

$$d + by + az = 0$$

which leads to $a^2 + ab + ad + bd = 0$, which is impossible or

$$d + by + az = d + cx$$

which leads to $a^2 + ab + ac + ad = 0$, which is also impossible. Note that the other assumption of equation on third or fourth elements leads to the same discussion above. Similarly, assuming $\mathbf{c_1} = 0$, $\mathbf{c_2} = 0$ and $\mathbf{c_3} = 0$ and following similar iterations of solving equations, we get the relations $a(a+b+c+d) = a^2+b^2$, $c(a+b+c+d) = c^2+d^2$ and

$$d(a+b+c+d) = c^2 + d^2 \tag{10}$$

respectively.

Subcase 1.2: $\hat{\mathbf{c}}$ is full non-zero, $\hat{\mathbf{c}'}$ has at most 2 zeros

Then we have at least two equations holds for non-zero elements. Assume they are the first two, then $c + ay + bz = 0$ and $d + by + az = 0$. Otherwise there are three equal elements from $\hat{\mathbf{c}}$ and $\hat{\mathbf{c}'}$, which contradicts the MDS property, as the input has 3 non-zero elements and output has only 1 non-zero element. We have

$$\begin{cases} a + bx = a + cy + dz \\ b + ax = b + dy + cz \\ 0 = c + ay + bz \end{cases} \tag{11}$$

which leads to the solution of

$$\begin{cases} x = \frac{c(c^2+d^2)}{d(a^2+b^2)} \\ y = \frac{c(ad+bc)}{d(a^2+b^2)} \\ z = \frac{c(ac+bd)}{d(a^2+b^2)} \end{cases}$$

substitute the value of x, y, z into the last elements of $\hat{\mathbf{c}}, \hat{\mathbf{c}'}$, combining with

$$d + by + az = 0$$

leads to $ad + bd + ac + bc = 0$, which is impossible.
Other assumptions like first and third elements equal leads to the system

$$\begin{cases} a + bx = a + cy + dz \\ 0 = b + dy + cz \\ c + dx = c + ay + bz \\ 0 = d + by + az \end{cases} \tag{12}$$

which leads to condition $b^2+d^2 = ab+cd$. This relation shows equivalence with the relations of $(\mathsf{wt}(\hat{\mathbf{b}}), \mathsf{wt}(\hat{\mathbf{b}'})) = (2,2)$ case. This is because we have $\mathsf{wt}(\hat{\mathbf{b}} + \hat{\mathbf{b}'}) = 3$ and $\mathsf{wt}(\hat{\mathbf{c}} + \hat{\mathbf{c}'}) = 2$. Therefore, the differential $(\hat{\mathbf{c}'}, \hat{\mathbf{c}} + \hat{\mathbf{c}'})$ can be viewed as the case $(\mathsf{wt}(\hat{\mathbf{b}}), \mathsf{wt}(\hat{\mathbf{b}'})) = (2,2)$ over M^{-1}. Due to this equivalence, we omit discussing similar cases.

3.2.2 Case 2: $\hat{\mathbf{b}} = [1, 0, x, 0]$ and $\hat{\mathbf{b}'} = [1, y, 0, z]$

We have $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}} = [a+cx, b+dx, c+ax, d+bx]$ and $\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'} = [a+by+dz, b+ay+cz, c+dy+bz, d+cy+az]$. If we swap b and c, and exchange second and third elements of $\hat{\mathbf{c}}$ and $\hat{\mathbf{c}'}$, it results in Case 1. See table 3 for relations.

Table 3: Relations for $\hat{\mathbf{b}} = [1, 0, x, 0]$ and $\hat{\mathbf{b}'} = [1, y, 0, z]$

Iterations	Steps	Results
$\mathbf{c_0} = 0 \implies x = \frac{a}{c}$	Solve unknowns in: $\mathbf{c'_2} = \mathbf{c_2}, \mathbf{c'_1} = 0$ Substitute in:$\mathbf{c'_3} = 0$	$c(a+b+c+d) = a^2 + c^2$
$\mathbf{c_1} = 0 \implies x = \frac{b}{d}$	Solve unknowns in: $\mathbf{c'_3} = \mathbf{c_3}, \mathbf{c'_0} = 0$ Substitute in: $\mathbf{c'_2} = 0$	$d(a+b+c+d) = b^2 + d^2$
$\mathbf{c_2} = 0 \implies x = \frac{c}{a}$	Solve unknowns in: $\mathbf{c'_0} = \mathbf{c_0}, \mathbf{c'_3} = 0$ Substitute in:$\mathbf{c'_1} = 0$	$a(a+b+c+d) = a^2 + c^2$
$\mathbf{c_3} = 0 \implies x = \frac{d}{b}$	Solve unknowns in: $\mathbf{c'_1} = \mathbf{c_1}, \mathbf{c'_2} = 0$ Substitute in: $\mathbf{c'_0} = 0$	$b(a+b+c+d) = b^2 + d^2$

3.2.3 Case 3: $\hat{\mathbf{b}} = [1, 0, 0, x]$ and $\hat{\mathbf{b}'} = [1, z, y, 0]$

We have $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}} = [a+dx, b+cx, c+bx, d+ax]$ and $\hat{\mathbf{c}'} = M \cdot \hat{\mathbf{b}'} = [a+bz+cy, b+az+dy, c+dz+ay, d+cz+by]$. If we swap b and d, and exchange second and fourth elements of $\hat{\mathbf{c}}$ and $\hat{\mathbf{c}'}$, it results in Case 1. See table 4 for relations.

Table 4: Relations for $\hat{\mathbf{b}} = [1, 0, 0, x]$ and $\hat{\mathbf{b}'} = [1, z, y, 0]$

Iterations	Steps	Results
$\mathbf{c_0} = 0 \implies x = \frac{a}{d}$	Solve unknowns in: $\mathbf{c'_3} = \mathbf{c_3}, \mathbf{c'_1} = 0$ Substitute in:$\mathbf{c'_2} = 0$	$d(a+b+c+d) = a^2 + d^2$
$\mathbf{c_1} = 0 \implies x = \frac{b}{c}$	Solve unknowns in: $\mathbf{c'_2} = \mathbf{c_2}, \mathbf{c'_0} = 0$ Substitute in: $\mathbf{c'_3} = 0$	$c(a+b+c+d) = b^2 + c^2$
$\mathbf{c_2} = 0 \implies x = \frac{c}{b}$	Solve unknowns in: $\mathbf{c'_1} = \mathbf{c_1}, \mathbf{c'_3} = 0$ Substitute in:$\mathbf{c'_0} = 0$	$b(a+b+c+d) = b^2 + c^2$
$\mathbf{c_3} = 0 \implies x = \frac{d}{a}$	Solve unknowns in: $\mathbf{c'_0} = \mathbf{c_0}, \mathbf{c'_2} = 0$ Substitute in: $\mathbf{c'_1} = 0$	$a(a+b+c+d) = a^2 + d^2$

This concludes the identification of the next 12 relations indicating admittance of related differentials with $(\mathsf{wt}(\hat{\mathbf{b}}), \mathsf{wt}(\hat{\mathbf{b}'})) = (2, 3)$.

3.3 Analysis When $\mathsf{wt}(\hat{\mathbf{b}}) = 1$ and $\mathsf{wt}(\hat{\mathbf{b}'}) = 4$

We can move the same non-zero element to the first index that is

1. $\hat{\mathbf{b}} = [w, 0, 0, 0]$ and $\hat{\mathbf{b}'} = [w, x, y, z]$, which can be simplified to $\hat{\mathbf{b}} = [1, 0, 0, 0]$ and $\hat{\mathbf{b}'} = [1, x', y', z']$.

where x, y, z, w are unknowns which takes elements from $\mathbb{F}_{2^n}$.

3.3.1 Case 1: $\hat{\mathbf{b}} = [1, 0, 0, 0]$ and $\hat{\mathbf{b}'} = [1, x, y, z]$

We have $\hat{\mathbf{c}} = [a, b, c, d]$ and $\hat{\mathbf{c}'} = [a+bx+cy+dz, b+ax+dy+cz, c+dx+ay+bz, d+cx+by+az]$. Because $\hat{\mathbf{c}}$ is full non-zero from MDS property and $\hat{\mathbf{c}'}$ has at most 2 non-zero elements, here we discuss the two subcases seperately.

Subcase 1.1: $\hat{\mathbf{c}'}$ has 1 non-zero element

Assume it is $\mathbf{c_0'} = a + bx + cy + dz$, then we have

$$\begin{cases} a = a + bx + cy + dz \neq 0 \\ 0 = b + ax + dy + cz \\ 0 = c + dx + ay + bz \\ 0 = d + cx + by + az \end{cases} \tag{13}$$

which leads to $b^2 + ab + bc + bd + ac + ad = 0$ or $(a + b)(b + c + d) = 0$, so that

$$b + c + d = 0 \tag{14}$$

is the condition to be satisfied. Similarly, solving for $\mathbf{c_1'} \neq 0$,$\mathbf{c_2'} \neq 0$,$\mathbf{c_3'} \neq 0$, we get the relations $a + c + d = 0$, $a + b + d = 0$ and $a + b + c = 0$ respectively.

Subcase 1.2: $\hat{\mathbf{c}'}$ has 2 non-zero elements

Assume it is $a + bx + cy + dz$ and $b + ax + dy + cz$, then we have

$$\begin{cases} a = a + bx + cy + dz \neq 0 \\ b = b + ax + dy + cz \\ 0 = c + dx + ay + bz \\ 0 = d + cx + by + az \end{cases} \tag{15}$$

which leads to $ac + ad + bc + bd = 0$, which is impossible.

This gives us the list $\mathbf{R}$ with all the necessary and sufficient 28 equations. □

3.4 Completeness of Proofs

We briefly clarify why our case analysis in the proof of Theorem 3 exhausts all possible ways for a 4 × 4 Hadamard MDS matrix M to admit related differentials, thereby ensuring that the final list of 28 conditions is both necessary and sufficient.

3.4.1 Bounding Lemmas and Weight Constraints.

By Lemma 1 (due to Daemen and Rijmen), for related differentials $(\hat{\mathbf{b}}, \hat{\mathbf{c}})$ and $(\hat{\mathbf{b}'}, \hat{\mathbf{c}'})$ in an $m \times m$ MDS setting, it holds that

$$\min\Big\{\mathsf{wt}(\hat{\mathbf{b}}) + \mathsf{wt}(\hat{\mathbf{c}}),\ \mathsf{wt}(\hat{\mathbf{b}'}) + \mathsf{wt}(\hat{\mathbf{c}'}),\ \mathsf{wt}(\hat{\mathbf{b}} \oplus \hat{\mathbf{b}'}) + \mathsf{wt}(\hat{\mathbf{c}} \oplus \hat{\mathbf{c}'})\Big\} \ \leq\ m + \left\lfloor \tfrac{m}{3} \right\rfloor.$$

For $m = 4$, at least one of these sums must be at most 5. In our analysis, this means we may focus on input–output differences whose combined weight does not exceed 5. Moreover, Lemma 3 shows that input pairs with weights $(1, 1)$ and $(1, 2)$ cannot yield related differentials when $m = 4$. Consequently, the *only* input difference pairs that remain relevant for a 4 × 4 Hadamard MDS matrix are those with weights $(1, 4)$, $(2, 2)$, or $(2, 3)$. As we illustrate below, examining these pairs (and their corresponding outputs) naturally leads to the generalized input–output relations that underlie our final set of 28 conditions.

3.4.2 Case-by-Case Enumeration.

For each weight class, we enumerate *all* relevant input pairs up to field scalings and coordinate permutations. For instance, an input vector with weight 2 is scaled so that its first nonzero entry becomes 1, and we systematically place the second nonzero entry in positions 2, 3, or 4. A similar strategy applies for weight 3 and weight 4 vectors. Consequently, we reduce each scenario to a canonical form (*e.g.*, $\hat{\mathbf{b}} = [1, 0, 0, x]$, etc.) without losing any potential relatedness conditions.

3.4.3 Output Polynomial Constraints.

For each enumerated input pair, we compute the outputs $\hat{\mathbf{c}} = M \cdot \hat{\mathbf{b}}$, $\hat{\mathbf{c'}} = M \cdot \hat{\mathbf{b'}}$, and impose the "related difference" requirement on these outputs (Definition 1). This leads to polynomial equations in the matrix elements $\{a, b, c, d\}$. By collecting and merging duplicates, we ultimately arrive at exactly 28 *distinct* constraints (Section 3, Theorem 3).

3.4.4 Necessity.

Necessity follows from the fact that any valid related differential pair, by the bounding lemma, must appear in our enumerations. Hence if M truly admits a related differential, at least one of those 28 constraints must hold.

3.4.5 Sufficiency.

Sufficiency is immediate: once a constraint is satisfied, we can exhibit a corresponding input pair $(\hat{\mathbf{b}}, \hat{\mathbf{b'}})$ whose outputs are related differentials. We could divide 28 equations from Theorem 3 into 3 distinct classes:

Class 1: When Equation 2 holds

Given condition:

$$ab + cd = b^2 + c^2.$$

Choice of the input differentials:

$$\hat{\mathbf{b}} = [1, 0, 0, \frac{c}{b}], \hat{\mathbf{b'}} = [0, \frac{c^3 + c(b^2 + d^2) + abd}{b(ac + bd)}, \frac{b^3 + b(a^2 + c^2) + acd}{b(ac + bd)}, 0].$$

Resulting outputs:

$$\hat{\mathbf{c}} = [a + \frac{cd}{b}, b + \frac{c^2}{b}, 0, d + \frac{ac}{b}],$$

$$\begin{aligned}\hat{\mathbf{c'}} &= [\frac{(ac + bd)(ab + cd)}{b(ac + bd)}, \frac{(ac + bd)(b^2 + c^2)}{b(ac + bd)}, \frac{(ab + cd)(a^2 + b^2 + c^2 + d^2)}{b(ac + bd)}, \frac{b^4 + c^4 + a^2b^2 + c^2d^2}{b(ac + bd)}] \\ &= [a + \frac{cd}{b}, b + \frac{c^2}{b}, 0, \frac{(b^2 + c^2 + ab + cd)^2)}{b(ac + bd)}] \\ &= [a + \frac{cd}{b}, b + \frac{c^2}{b}, 0, 0].\end{aligned}$$

Since $\hat{\mathbf{c}}$ and $\hat{\mathbf{c'}}$ are related differentials, M admits related differentials.

Class 2: When Equation 10 holds

Given conditions:

$$d(a + b + c + d) = c^2 + d^2,$$

i.e.,

$$c^2 + ad + bd + cd = 0.$$

Choice of the input differentials:

$$\hat{\mathbf{b}} = [1, \frac{d}{c}, 0, 0], \hat{\mathbf{b'}} = [1, 0, \frac{d(ad + bc)}{c(c^2 + d^2)}, \frac{d(ac + bd)}{c(c^2 + d^2)}].$$

Resulting outputs:

$$\hat{\mathbf{c}} = [a + \frac{bd}{c}, b + \frac{ad}{c}, c + \frac{d^2}{c}, 0],$$

$$\begin{aligned}\hat{\mathbf{c}'} &= [\frac{(c^2+d^2)(ac+bd)}{c(c^2+d^2)}, \frac{(c^2+d^2)(ad+bc)}{c(c^2+d^2)}, \frac{c^4+c^2d^2+a^2d^2+b^2d^2}{c(c^2+d^2)}, \frac{cd(a^2+b^2+c^2+d^2)}{c(c^2+d^2)}]\\ &= [a+\frac{bd}{c}, b+\frac{ad}{c}, \frac{(c^2+cd+ad+bd)^2}{c(c^2+d^2)}, \frac{d(a^2+b^2+c^2+d^2)}{c^2+d^2}]\\ &= [a+\frac{bd}{c}, b+\frac{ad}{c}, 0, \frac{d(a^2+b^2+c^2+d^2)}{c^2+d^2}].\end{aligned}$$

Since $\hat{\mathbf{c}}$ and $\hat{\mathbf{c}'}$ are related differentials, M admits related differentials.

Class 3: When Equation 14 holds

Given conditions:

$$b+c+d=0,$$

i.e.,

$$(b+c+d)^2 = b^2+c^2+d^2 = 0.$$

Choice of the input differentials:

$$\hat{\mathbf{b}} = [1,0,0,0], \hat{\mathbf{b}'} = [1, \frac{b}{a}, \frac{c}{a}, \frac{d}{a}].$$

Resulting outputs:

$$\hat{\mathbf{c}} = [a,b,c,d],$$

$$\begin{aligned}\hat{\mathbf{c}'} &= [\frac{a^2+b^2+c^2+d^2}{a}, 0, 0, 0]\\ &= [a,0,0,0].\end{aligned}$$

Since $\hat{\mathbf{c}}$ and $\hat{\mathbf{c}'}$ are related differentials, M admits related differentials.

Thus, our coverage of low-weight pairs is *complete* for detecting related differentials, and the 28 resulting relations precisely characterize when a 4×4 Hadamard MDS matrix M over $\mathbb{F}_{2^n}$ admits related differentials.

4 Construction of 4×4 Hadamard MDS Matrices resistant to Related Differentials

To construct Hadamard MDS matrices resistant to related differentials, we can leverage the MDS property and Theorem 3. For any non-zero triplet (a,d,c), the necessary conditions are

$$\begin{cases} a \neq d \\ a \neq c \\ d \neq c \\ a+c+d \neq 0 \end{cases}$$

derived from 2×2 submatrices containing a, d, c and $a+b+c+d \neq b$. The choices for b are then constrained by the remaining MDS conditions and the 28 conditions from Theorem 3, consisting of linear and quadratic inequalities on b. The linear inequalities forms a set $\{a, d, c, a+c+d, \frac{ad}{c}, \frac{ac}{d}, \frac{cd}{a}, \frac{a^2+c^2+cd}{a}, \frac{a^2+d^2+cd}{a}, \frac{a^2+d^2+ac}{d}, \frac{c^2+d^2+ac}{d}, \frac{a^2+c^2+ad}{c}, \frac{c^2+d^2+ad}{c}, \frac{c^2+ac+ad}{a}, \frac{d^2+ac+ad}{a}, \frac{a^2+ac+cd}{c}, \frac{d^2+ac+cd}{c}, \frac{a^2+cd+ad}{d}, \frac{c^2+cd+ad}{d}, \frac{a^2}{a+c+d}, \frac{c^2}{a+c+d}, \frac{d^2}{a+c+d}, c+d, a+d, a+c\}$. Note that the set may contain multiple identical elements.

4.1 4×4 MDS Matrices over $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^4}$

When the entries of matrices belong to $\mathbb{F}_{2^3}$ or $\mathbb{F}_{2^4}$, the linear inequalities and quadratic inequalities consistently constitute a complete set of $\mathbb{F}^{\star}_{2^3}$ or $\mathbb{F}^{\star}_{2^4}$, irrespective of the specific values taken by the triplet (a, d, c). Therefore, all the matrices over these given fields have related differentials.

4.2 4×4 MDS Matrices over $\mathbb{F}_{2^n}$ with $n > 4$

When the entries of matrices belong to $\mathbb{F}_{2^n}$ with $n > 4$, the cardinality of values resulting from the combined constraints of linear and quadratic inequalities will be less than $2^n - 1$. Consequently, b can assume values arbitrarily from the set of $\mathbb{F}_{2^n}$, excluding invalid values calculated from those inequalities.

4.3 Exhaustive List of All Resistant 4×4 MDS Hadamard Matrices over $\mathbb{F}_{2^n}$ with $n > 4$

Let us denote by $\mathcal{M}_{free}$ the exhaustive list of all 4×4 Hadamard matrices T where the elements of T do not satisfy any of the equations in $\mathbf{R}$ found in Theorem 3 and hence are resistant to related differentials. The list $\mathcal{M}_{free}$ is generated using Algorithm 1.

Algorithm 1 Generation of the list $\mathcal{M}_{free}$

```
Require: An extension field $\mathbb{F}_{2^n}$.
Ensure: The collection $\mathcal{M}_{free}$ of all $4 \times 4$ Hadamard matrices $T$ over $\mathbb{F}_{2^n}$ that are both
    MDS and do not satisfy any equations in $\mathbf{R}$.
$\mathcal{M}_{free} \leftarrow \varnothing$                    ▷ Initialize empty list of resistant matrices
for all $(a, b, c, d) \in (\mathbb{F}_{2^n} \setminus \{0\})^4$ do
    Construct the $4 \times 4$ Hadamard matrix $T$ using $\{a, b, c, d\}$.
    if $T$ is MDS then
        if $\{a, b, c, d\}$ do not satisfy any equation in $\mathbf{R}$ then
            $\mathcal{M}_{free} \leftarrow \mathcal{M}_{free} \cup \{T\}$                    ▷ Store $T$
        end if
    end if
end for
return $\mathcal{M}_{free}$
```

We can view $\mathcal{M}_{free}$ as a collection of sub-lists, say $\mathcal{M}_i$, where $i = 1, 2, \ldots, 2^n - 1$ and each of these sub-lists consist of matrices T with $T[0, 0] = i$. Running the aforementioned steps for the case of matrices over $\mathbb{F}_{2^8}$ through a simple C code[2] reveals that the total number of resistant matrices in each sub-list is exactly 14229600. For the matrices over $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^6}$, each sub-list has 5040 and 127176 resistant matrices respectively. *Note that* Algorithm 1 drastically reduces the complexity of verifying whether a matrix T admits related differentials or not, compared to the traditional brute-force approach where one needs to check all possible pairs of input and the corresponding output differences to see if they satisfy the related differential property stated in Definition 2. For example, with a traditional brute-force approach, verifying the presence of related differentials in a matrix T over $\mathbb{F}_{2^4}$ would require 840^2 checks on all input and corresponding output pairs, where input and output differences have combined weight of 5 (due to Lemma 1). Similar verification for matrices over $\mathbb{F}_{2^5}$, $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^8}$ would require 1736^2, 3528^2 and 14280^2 checks on all input and output pairs respectively. Moreover, the brute-force verification

[2] Source codes available on https://github.com/sjsonucool/hadamard-matrices-resistant-to-related-differentials-cryptanalysis.

complexity would increase further for matrices over $\mathbb{F}_{2^n}$ with $n > 8$. However, due to the consequence of Theorem 3, step 5 of Algorithm 1 only checks if the elements of a 4×4 matrix T over any field $\mathbb{F}_{2^n}$ satisfies any of the 28 relations deduced from Theorem 3.

Equivalence classes over related differentials: In order to exhaustively generate the list of resistant MDS matrices, it suffices to only generate all the matrices T (with $T[0,0] = 1$) contained in the sub-list $\mathcal{M}_1$ using the aforementioned steps. The matrices in the rest of the sub-lists with $T[0,0] = i, (i \neq 1)$ are the multiplication of matrices contained in $\mathcal{M}_1$ with scalar i. Consider a quartet of differences $\{\hat{\mathbf{x}}, \hat{\mathbf{x}'}, T(\hat{\mathbf{x}}), T(\hat{\mathbf{x}'})\}$ where $T(\hat{\mathbf{x}})$ denotes post-multiplication of vector $\hat{\mathbf{x}}$ with matrix T. The differentials $(\hat{\mathbf{x}}, T(\hat{\mathbf{x}}))$ and $(\hat{\mathbf{x}'}, T(\hat{\mathbf{x}'}))$ are related, if and only if the differentials $(\alpha \cdot \hat{\mathbf{x}}, T(\alpha \cdot \hat{\mathbf{x}}))$ and $(\alpha \cdot \hat{\mathbf{x}'}, T(\alpha \cdot \hat{\mathbf{x}'}))$ are related for any $\alpha \in \mathbb{F}_{2^n}^*$. Consider a matrix T such that $T[0,0] = \alpha$. If $\{\hat{\mathbf{x}}, \hat{\mathbf{x}'}, T(\hat{\mathbf{x}}), T(\hat{\mathbf{x}'})\}$ denotes a related difference pair for the map T, then the quartet $(\alpha \cdot \hat{\mathbf{x}}, T(\alpha \cdot \hat{\mathbf{x}}))$ and $(\alpha \cdot \hat{\mathbf{x}'}, T(\alpha \cdot \hat{\mathbf{x}'}))$ are also a related difference pair for the matrix $\alpha^{-1} \cdot T \in \mathcal{M}_1$. Therefore, if we have generated the list of all resistant matrices in $\mathcal{M}_1$, then consequently we have found all the resistant matrices over $\mathbb{F}_{2^n}$. Note that this property holds for any MDS matrix, regardless of the matrix structure and dimension.

4.4 Searching Lightweight Matrices in $\mathcal{M}_1$

In [BKL16], the authors address the problem of identifying an optimal implementation for the multiplication of a given field element over $\mathbb{F}_{2^n}$. They present tables with minimal XOR counts for multiplication with elements in $\mathbb{F}_{2^n}$. We utilize the table for elements in $\mathbb{F}_{2^8}$ from [BKL16, p. 650] to search for lightweight matrices in $\mathcal{M}_1$ with respect to the minimal XOR count.

We consider a 4×4 matrix whose first row is $[a \quad b \quad c \quad d]$, while the remaining rows follow a Hadamard permutation structure. When this matrix is multiplied by a vector $[x \quad y \quad z \quad w]^T$, it produces four output elements in $\mathbb{F}_{2^8}$, calculated as:

$$\begin{aligned}
\text{Output}_1 &= a \cdot x \oplus b \cdot y \oplus c \cdot z \oplus d \cdot w, \\
\text{Output}_2 &= a \cdot y \oplus b \cdot x \oplus c \cdot w \oplus d \cdot z, \\
\text{Output}_3 &= a \cdot z \oplus b \cdot w \oplus c \cdot x \oplus d \cdot y, \\
\text{Output}_4 &= a \cdot w \oplus b \cdot z \oplus c \cdot y \oplus d \cdot x.
\end{aligned}$$

To compute the XOR cost of this matrix, we refer to the XOR cost associated with the multiplications by the matrix elements $\{a, b, c, d\}$. Using the minimal XOR counts provided in the table mentioned above, we define the bitwise cost of multiplying by an element x as $\text{cost}(x)$. Since each of a, b, c, d appears exactly once in all four output terms, the total multiplication cost is calculated as

$$4 \times \big(\text{cost}(a) + \text{cost}(b) + \text{cost}(c) + \text{cost}(d)\big).$$

Furthermore, each output element, for instance $\text{Output}_1 = a \cdot x \oplus b \cdot y \oplus c \cdot z \oplus d \cdot w$, requires three XOR operations to combine the four terms. With four output elements, the additional number of XOR operations is $4 \times 3 = 12$. As each XOR operation in $\mathbb{F}_{2^8}$ requires 8 bitwise XOR gates, these 12 operations result in $12 \times 8 = 96$ XOR gates. Consequently, the total XOR gate cost is

$$4\big(\text{cost}(a) + \text{cost}(b) + \text{cost}(c) + \text{cost}(d)\big) \; + \; 96.$$

For matrices in $\mathcal{M}_1$, the minimum multiplication cost with respect to the XOR count is 120. Table 13 presents a list of 20 matrices in $\mathcal{M}_1$ that achieve this minimum cost. The corresponding inverse matrices and their respective costs are also listed in this table.

The method from [BKL16] provides a means of computing the XOR costs of binary matrices (see Appendix D for brief description on forming binary multiplication matrices from field elements and check the respective code for forming binary matrices provided on GitHub).

However, subsequent research has introduced more advanced techniques for optimizing XOR cost calculation. In particular, the work of [XZL$^+$20] presents a heuristic approach for matrix decomposition that achieves lower XOR costs than previous heuristics. While this paper does not explicitly focus on the detailed computation of XOR costs from binary matrices, we encourage readers with an interest in this topic to refer to [XZL$^+$20] for a thorough description of their methodology. Additionally, our current work does not aim to compute or identify the lightest Hadamard MDS matrices resistant to related differentials, as that is outside the scope of this study. Instead, we provide practical insights into the XOR cost analysis, motivated by the small set of matrices presented in Tables 15. The table serve as a valuable starting point for future research into lightweight optimizations and cost-effective methods in XOR computation of Hadamard matrices free of related differentials.

5 Related Differentials Properties over 8×8 Hadamard MDS Matrices

We have demonstrated a deterministic construction of 4×4 Hadamard MDS matrices over $\mathbb{F}_{2^n}$ that are free of related differentials. A natural extension of the study is to analyze the properties of related differentials and to construct 8×8 Hadamard MDS matrices over $\mathbb{F}_{2^n}$ that are also free of related differentials. For an arbitrary n, however, the exhaustive search for an 8×8 matrix without related differentials becomes increasingly infeasible due to the huge size of the matrix set. Therefore, constructing such matrices deterministically for any n requires a complete characterization of the relations that the elements of the matrix must not satisfy. The methodology outlined in Section 3 becomes highly complicated and cumbersome when extended to 8×8 matrices. Developing a more compact and efficient approach to analyze and deduce the set of relations for 8×8 matrices remains an open problem. Nevertheless, in this section, we propose experimental methods incorporating faster search and verification techniques to determine if a given 8×8 Hadamard MDS matrix over $\mathbb{F}_{2^n}$ admits related differentials. Using these methods, we have verified that all the matrices in the sets $\mathbb{F}_{2^4}^{8\times 8}$ and $\mathbb{F}_{2^5}^{8\times 8}$ consist of related differentials.

From [PSA$^+$18], it is established that a Hadamard matrix $M \in \mathbb{F}_{2^n}^{k\times k}$, formed using elements $\{a_0, a_1, \ldots, a_{k-1}\}$ such that $M_{i,j} = a_{i\oplus j}$, satisfies the properties $M = M^T$ and $M^2 = s^2 \cdot I_k$, where $s = \bigoplus_{i=0}^{k-1} a_i$ is a scalar, and I_k is the $k \times k$ identity matrix.

Theorem 4. *Let M be an invertible $k \times k$ Hadamard matrix with entries in $\mathbb{F}_{2^n}$. Define s as the (nonzero) XOR sum of the elements in the first row of M, given by*

$$s = \bigoplus_{i=0}^{k-1} a_i,$$

where $\{a_i\}$ are the entries of the first row of M. Let the matrix M' be obtained by scaling each entry of M by s^{-1} as

$$a_i' = a_i \cdot s^{-1}.$$

Then the scaled $k \times k$ Hadamard matrix M' is involutory.

Proof. Since M is a Hadamard matrix over $\mathbb{F}_{2^n}$, it satisfies

$$M^2 = s^2 I_k,$$

where

$$s \;=\; \bigoplus_{i=0}^{k-1} a_i,$$

and $s \neq 0$ because M is invertible.

We know that the matrix M' is formed as:

$$a'_i \;=\; a_i \,\cdot\, s^{-1}.$$

Hence, M' can be expressed as

$$M' \;=\; s^{-1}\, M,$$

where s^{-1} is the multiplicative inverse of s in $\mathbb{F}_{2^n}$. The involutory property of M' can be verified as

$$(M')^2 \;=\; (s^{-1}M)\,(s^{-1}M) \;=\; s^{-2}\, M^2 \;=\; s^{-2}\left(s^2 I_k\right) \;=\; I_k.$$

Thus, M' satisfies $(M')^2 = I_k$, proving that M' is an *involutory* matrix. □

Note that scaling the entries of M by s^{-1} preserves the symmetric Hadamard structure, as the relative relationships between the matrix entries remain unchanged under uniform scaling. Therefore, M' retains the Hadamard property and is the desired *involutory* Hadamard matrix of order k. We restate below the theorem on the equivalence classes of Hadamard matrices proposed in [SKOP15].

Theorem 5. *[SKOP15] Given a set of 2^t nonzero elements, $S = \{\alpha_0, \alpha_1, \ldots, \alpha_{2^t-1}\}$, there are $\frac{(2^t-1)!}{\prod_{i=0}^{t-1}(2^t-2^i)}$ equivalence classes of Hadamard matrices of order 2^t defined by the set of elements S.*

Based on Theorem 5, we observe that there are 30 equivalence classes of 8×8 matrices formed by the set S, which contains 8 elements. In [SKOP15], the authors present an algorithm to generate one representative matrix from each equivalence class, which is restated below (for detailed proofs of Theorem 5 and Algorithm 2, refer to the original paper).

Algorithm 2 Construction of candidate 8×8 Hadamard matrix entries [SKOP15]

Require: A sorted set of 8 distinct elements $\{\alpha_0, \alpha_1, \ldots, \alpha_7\}$ in ascending order.

```
$\alpha_0 \leftarrow$ the smallest element
$\alpha_1 \leftarrow$ the second smallest element
$\alpha_2 \leftarrow$ the third smallest element    ▷ Fix the first three entries.
$S \leftarrow \{\alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7\}$    ▷ The remaining 5 elements in ascending order.
for all $x \in S$ (in ascending order) do
    $\alpha_3 \leftarrow x$
    $S' \leftarrow S \setminus \{x\}$
    $\alpha_4 \leftarrow \min(S')$    ▷ Select the smallest of the remaining 4 elements as $\alpha_4$.
    $R \leftarrow S' \setminus \{\alpha_4\}$    ▷ Now $R$ contains the 3 leftover elements.
    for all permutations $(p_5, p_6, p_7)$ of $R$ do
        $(\alpha_5, \alpha_6, \alpha_7) \leftarrow (p_5, p_6, p_7)$    ▷ Assign the permuted elements as the last three entries.
        Form the candidate matrix $T$ from $\alpha_0, \ldots, \alpha_7$.
    end for
end for
```

Given Theorems 4, 5 and Algorithm 2, we propose Algorithm 3 to perform a faster search for matrices over $\mathbb{F}_{2^n}$ with related differentials. Note that due to Theorem 4, we only need to exhaustively check the set of involutory matrices for the presence of related differentials to verify the results for entire matrix set. This drastically reduces the search time compared to an exhaustive search over the entire matrix set $\mathbb{F}_{2^n}^{8\times 8}$.

Algorithm 3 Faster verification of related differentials in $\mathbb{F}_{2^n}^{8\times 8}$ using equivalence classes of Involutory Hadamard Matrices

```
Require: A finite field $\mathbb{F}_{2^n}$ of size $2^n$, where $n \in \mathbb{N}$.
                                                    ▷ Enumerate 7-element subsets
for all 7-element subsets $\{a, b, c, d, x, y, z\}$ of $(\mathbb{F}_{2^n} \setminus \{0\})$ do
                                                    ▷ Define the set $S$
    $S \leftarrow \{a, b, c, d, x, y, z, a \oplus b \oplus c \oplus d \oplus x \oplus y \oplus z \oplus 1\}$
    Using Algorithm 2, generate 30 non equivalent matrices from $S$ and store in $\mathcal{T}$
                                                    ▷ Verify MDS and RD properties of each matrix
    for all $T \in \mathcal{T}$ do
        if $T$ is MDS then
            Check if $T$ admits related differentials (RD) (definition 2).
        end if
    end for
end for
```

By performing experiments based on the steps outlined in Algorithm 3 on 8 × 8 involutory matrices with elements over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^5}$, we observe that no matrices in the sets $\mathbb{F}_{2^4}^{8\times 8}$ and $\mathbb{F}_{2^5}^{8\times 8}$ are free of related differentials. In fact, there is only one representative involutory matrix $\mathrm{had}(2, 3, 4, 12, 5, 10, 8, 15) \in \mathbb{F}_{2^4}^{8\times 8}$ which is MDS and admits related differentials, and there are 255 MDS representative involutory matrices in $\mathbb{F}_{2^5}^{8\times 8}$ each of which admits related differentials.

6 Conclusion

In this paper, we propose a deterministic approach for constructing MDS matrices that are resilient against related-differential cryptanalysis. Our primary focus is on the related-differentials property of linear layers, which can be exploited to attack block ciphers/hash functions, and under what conditions matrices used in such layers do not admit this property. Using Hadamard MDS matrices as a basis of our study, we present methods for constructing 4×4 Hadamard MDS matrices over $\mathbb{F}_{2^n}$ that are devoid of related differentials, accompanied by concrete proofs. These proposed methods are feasible and can also be incorporated in other matrix structures to determine the conditions in which they admit related differentials, and consequently filter the matrices devoid of related differentials. Additionally, we propose faster search and verification techniques to identify if the matrices in the set $\mathbb{F}_{2^n}^{8\times 8}$ exhibit related differentials. To the best of our knowledge, this paper for the first time adds a new direction towards the construction of MDS matrices with focus on their resistance towards differential cryptanalysis, when incorporated in AES-like ciphers.

References

[AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology (NIST), FIPS PUB 197, U.S. Department of Commerce, November 2001.

[AF14] Daniel Augot and Matthieu Finiasz. Direct construction of recursive mds diffusion layers using shortened bch codes. In *Fast Software Encryption: 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers 21*, pages 3–17. Springer, 2014. doi:10.1007/978-3-662-46706-0_1.

[Ber13] Thierry P Berger. Construction of recursive mds diffusion layers from gabidulin codes. In *Progress in Cryptology–INDOCRYPT 2013: 14th International Conference on Cryptology in India, Mumbai, India, December 7-10, 2013. Proceedings 14*, pages 274–285. Springer, 2013. doi:10.1007/978-3-319-03515-4_18.

[BKL16] Christof Beierle, Thorsten Kranz, and Gregor Leander. Lightweight multiplication in gf(2ˆn) with applications to MDS matrices. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 625–653. Springer, 2016. doi:10.1007/978-3-662-53018-4_23.

[BR00] Paulo Barreto and Vincent Rijmen. The Anubis block cipher. First open NESSIE Workshop, Leuven, 2000. https://tinyurl.com/3bnfnekc.

[CLM16] Victor Cauchois, Pierre Loidreau, and Nabil Merkiche. Direct construction of quasi-involutory recursive-like mds matrices from 2-cyclic codes. *IACR Transactions on Symmetric Cryptology*, 2016. doi:10.13154/TOSC.V2016.I2.80-98.

[DL18] Sébastien Duval and Gaëtan Leurent. MDS matrices with lightweight circuits. *IACR Trans. Symmetric Cryptol.*, 2018(2):48–78, 2018. doi:10.13154/tosc.v2018.i2.48-78.

[DR02] Joan Daemen and Vincent Rijmen. The design of rijndael: Aes-the advanced encryption standard. *Information Security and Cryptography*, 2002. doi:10.1007/978-3-662-04722-4.

[DR09] Joan Daemen and Vincent Rijmen. New Criteria for Linear Maps in AES-like Ciphers. *Cryptogr. Commun.*, 1(1):47–69, 2009. doi:10.1007/s12095-008-0003-x.

[GBR22] Navid Ghaedi Bardeh and Vincent Rijmen. New key-recovery attack on reduced-round aes. *IACR Transactions on Symmetric Cryptology*, 2022(2):43–62, Jun. 2022. URL: https://tosc.iacr.org/index.php/ToSC/article/view/9713, doi:10.46586/tosc.v2022.i2.43-62.

[GPP11] Jian Guo, Thomas Peyrin, and Axel Poschmann. The photon family of lightweight hash functions. In *Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings 31*, pages 222–239. Springer, 2011. doi:10.1007/978-3-642-22792-9_13.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw. The led block cipher. In *Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13*, pages 326–341. Springer, 2011. doi:10.1007/978-3-642-23951-9_22.

[GPV17] Kishan Chand Gupta, Sumit Kumar Pandey, and Ayineedi Venkateswarlu. Towards a general construction of recursive mds diffusion layers. *Designs, Codes and Cryptography*, 82:179–195, 2017. doi:10.1007/S10623-016-0261-0.

[JPST17] Jérémy Jean, Thomas Peyrin, Siang Meng Sim, and Jade Tourteaux. Optimizing implementations of lightweight building blocks. *IACR Trans. Symmetric Cryptol.*, 2017(4):130–168, 2017. doi:10.13154/tosc.v2017.i4.130-168.

[KLSW17] Thorsten Kranz, Gregor Leander, Ko Stoffelen, and Friedrich Wiemer. Shorter linear straight-line programs for mds matrices. *IACR Transactions on Symmetric Cryptology*, pages 188–211, 2017. doi:10.13154/TOSC.V2017.I4.188-211.

[LS16] Meicheng Liu and Siang Meng Sim. Lightweight MDS generalized circulant matrices. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 101–120. Springer, 2016. doi:10.1007/978-3-662-52993-5_6.

[LSL+19] 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, 2019. doi:10.13154/TOSC.V2019.I1.84-117.

[LSS+20] Shun Li, Siwei Sun, Danping Shi, Chaoyun Li, and Lei Hu. Lightweight iterative mds matrices: How small can we go? *IACR Transactions on Symmetric Cryptology*, 2019, Issue 4:147–170, 2020. URL: https://tosc.iacr.org/index.php/ToSC/article/view/8460, doi:10.13154/tosc.v2019.i4.147-170.

[LW16] Yongqiang Li and Mingsheng Wang. On the construction of lightweight circulant involutory MDS matrices. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 121–139. Springer, 2016. doi:10.1007/978-3-662-52993-5_7.

[LW17] Chaoyun Li and Qingju Wang. Design of lightweight linear diffusion layers from near-mds matrices. *IACR Trans. Symmetric Cryptol.*, 2017(1):129–155, 2017. doi:10.13154/tosc.v2017.i1.129-155.

[MS77] F. Jessie MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier, 1977. URL: https://api.semanticscholar.org/CorpusID:118260868.

[PSA+18] Meltem Kurt Pehlivanoğlu, Muharrem Tolga Sakallı, 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. URL: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-ifs.2017.0156, arXiv:https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/iet-ifs.2017.0156, doi:10.1049/iet-ifs.2017.0156.

[RBH17] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo tricks with AES. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 217–243. Springer, Heidelberg, December 2017. doi:10.1007/978-3-319-70694-8_8.

[SKOP15] 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. doi:10.1007/978-3-662-48116-5_23.

[SS16a] Sumanta Sarkar and Siang Meng Sim. A deeper understanding of the XOR count distribution in the context of lightweight cryptography. In David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, volume 9646 of *Lecture Notes in Computer Science*, pages 167–182. Springer, 2016. doi:10.1007/978-3-319-31517-1_9.

[SS16b] Sumanta Sarkar and Habeeb Syed. Lightweight diffusion layer: Importance of toeplitz matrices. *IACR Trans. Symmetric Cryptol.*, 2016(1):95–113, 2016. doi:10.13154/tosc.v2016.i1.95-113.

[SS17] Sumanta Sarkar and Habeeb Syed. Analysis of toeplitz MDS matrices. In Josef Pieprzyk and Suriadi Suriadi, editors, *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part II*, volume 10343 of *Lecture Notes in Computer Science*, pages 3–18. Springer, 2017. doi:10.1007/978-3-319-59870-3_1.

[TTKS18] Dylan Toh, Jacob Teo, Khoongming Khoo, and Siang Meng Sim. Lightweight mds serial-type matrices with minimal fixed xor count. In *Progress in Cryptology–AFRICACRYPT 2018: 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7–9, 2018, Proceedings 10*, pages 51–71. Springer, 2018. doi:10.1007/978-3-319-89339-6_4.

[WWW13] Shengbao Wu, Mingsheng Wang, and Wenling Wu. Recursive diffusion layers for (lightweight) block ciphers and hash functions. In Lars R. Knudsen and Huapeng Wu, editors, *SAC 2012*, volume 7707 of *LNCS*, pages 355–371. Springer, Heidelberg, August 2013. doi:10.1007/978-3-642-35999-6_23.

[XZL+20] Zejun Xiang, Xiangyong Zeng, Da Lin, Zhenzhen Bao, and Shasha Zhang. Optimizing implementations of linear layers. *IACR Trans. Symm. Cryptol.*, 2020(2):120–145, 2020. doi:10.13154/tosc.v2020.i2.120-145.

[ZWS18] Lijing Zhou, Licheng Wang, and Yiru Sun. On efficient constructions of lightweight MDS matrices. *IACR Trans. Symmetric Cryptol.*, 2018(1):180–200, 2018. doi:10.13154/tosc.v2018.i1.180-200.

A Examples of Hadamard MDS matrices in $\mathbb{F}_{2^8}^{4\times 4}$ Satisfying relations in Theorem 3

In this section we present a list of Hadamard MDS matrices $\{M_1, M_2, M_3, M_4\} \in \mathbb{F}_{2^8}^{4\times 4}$ along with their sets of related differentials. The related differentials for these matrices, omitting the hexadecimal representation prefix (0x), are listed in the Tables 5, 6, 7, and 8. Note that the multiplication of these related differentials by the scalar $\alpha \in \mathbb{F}_{2^8}^*$, are also related differentials. The total number of related differentials and the relations between matrix elements (in the form of $\{a, b, c, d\}$) for each matrix are shown in the Table 9. The irreducible polynomial for field multiplication is $x^8 + x^4 + x^3 + x + 1$. We begin by discussing a polynomial-form example of matrix-vector multiplication giving the first component of the output, using the matrix M_1 and the vector $\hat{\mathbf{b}} = [1, D6, 0, 0]$ shown in the first row of the Table 5. Same rule applies for other values of input-output pairs shown in the Tables 5, 6, 7, and 8.

The first component of the matrix-vector product over $\mathbb{F}_{2^8}$ is computed as:

$$\begin{pmatrix}\mathrm{F5} & \mathrm{5A} & 34 & \mathrm{3F}\end{pmatrix} \cdot \begin{pmatrix} 1 \\ \mathrm{D6} \\ 0 \\ 0 \end{pmatrix} = \mathrm{F5} \cdot 1 \oplus \mathrm{5A} \cdot \mathrm{D6}$$

- **F5** $= x^7 + x^6 + x^5 + x^4 + x^2 + 1$, multiplied by 1 remains unchanged
- **5A** $= x^6 + x^4 + x^3 + x$, multiplied by **D6** $= x^7 + x^6 + x^4 + x^2 + x$:

$$\begin{aligned}(x^6 + x^4 + x^3 + x)(x^7 + x^6 + x^4 + x^2 + x) &\equiv x^7 + x + 1 \pmod{x^8 + x^4 + x^3 + x + 1} \\ &\equiv 83_{16}\end{aligned}$$

- **Addition (XOR)**:

$$\begin{aligned}\mathrm{F5}_{16} \oplus 83_{16} &= (x^7 + x^6 + x^5 + x^4 + x^2 + 1) \\ &\quad \oplus (x^7 + x + 1) \\ &= x^6 + x^5 + x^4 + x^2 + x \\ &\equiv 76_{16}\end{aligned}$$

$$M_1 = \begin{bmatrix} \texttt{0xF5} & \texttt{0x5A} & \texttt{0x34} & \texttt{0x3F} \\ \texttt{0x5A} & \texttt{0xF5} & \texttt{0x3F} & \texttt{0x34} \\ \texttt{0x34} & \texttt{0x3F} & \texttt{0xF5} & \texttt{0x5A} \\ \texttt{0x3F} & \texttt{0x34} & \texttt{0x5A} & \texttt{0xF5} \end{bmatrix}, \qquad M_2 = \begin{bmatrix} \texttt{0x66} & \texttt{0x4D} & \texttt{0xBF} & \texttt{0x36} \\ \texttt{0x4D} & \texttt{0x66} & \texttt{0x36} & \texttt{0xBF} \\ \texttt{0xBF} & \texttt{0x36} & \texttt{0x66} & \texttt{0x4D} \\ \texttt{0x36} & \texttt{0xBF} & \texttt{0x4D} & \texttt{0x36} \end{bmatrix},$$

$$M_3 = \begin{bmatrix} \texttt{0x66} & \texttt{0x63} & \texttt{0x34} & \texttt{0xD2} \\ \texttt{0x63} & \texttt{0x66} & \texttt{0xD2} & \texttt{0x34} \\ \texttt{0x34} & \texttt{0xD2} & \texttt{0x66} & \texttt{0x63} \\ \texttt{0xD2} & \texttt{0x34} & \texttt{0x63} & \texttt{0x66} \end{bmatrix}, \qquad M_4 = \begin{bmatrix} \texttt{0x0F} & \texttt{0xDF} & \texttt{0xD0} & \texttt{0x75} \\ \texttt{0xDF} & \texttt{0x0F} & \texttt{0x75} & \texttt{0xD0} \\ \texttt{0xD0} & \texttt{0x75} & \texttt{0x0F} & \texttt{0xDF} \\ \texttt{0x75} & \texttt{0xD0} & \texttt{0xDF} & \texttt{0x0F} \end{bmatrix}.$$

Table 5: The sets of related differentials over M_1.

$\hat{\mathbf{b}}$	$\hat{\mathbf{c}}$	$\hat{\mathbf{b}'}$	$\hat{\mathbf{c}'}$
$[1, D6, 0, 0]$	$[76, 80, 80, 0]$	$[0, 0, D6, 1]$	$[0, 80, 80, 76]$
$[1, E2, 0, 0]$	$[67, 39, 0, 67]$	$[0, 0, E2, 1]$	$[67, 0, 39, 67]$
$[53, 16, 16, 0]$	$[1, D6, 0, 0]$	$[0, 16, 16, 53]$	$[0, 0, D6, 1]$
$[D8, 21, 0, D8]$	$[1, E2, 0, 0]$	$[D8, 0, 21, D8]$	$[0, 0, E2, 1]$

Table 6: The sets of related differentials over M_2

$\hat{\mathbf{b}}$	$\hat{\mathbf{c}}$	$\hat{\mathbf{b}'}$	$\hat{\mathbf{c}'}$
$[1, B1, 0, 0]$	$[63, AE, 0, AE]$	$[0, 0, 1, B1]$	$[0, AE, 63, AE]$
$[1, E0, 0, 0]$	$[54, 1A, 54, 0]$	$[0, 0, 1, E0]$	$[54, 0, 54, 1A]$
$[1, 0, 0, 63]$	$[89, 89, CD, 0]$	$[0, 1, 63, 0]$	$[89, 89, 0, CD]$
$[1, 0, 0, D3]$	$[0, AE, 85, 85]$	$[0, 1, D3, 0]$	$[AE, 0, 85, 85]$
$[8B, 15, 0, 15]$	$[1, B1, 0, 0]$	$[0, 15, 8B, 15]$	$[0, 0, 1, B1]$
$[CF, 6, CF, 0]$	$[1, E0, 0, 0]$	$[CF, 0, CF, 6]$	$[0, 0, 1, E0]$
$[FC, FC, 9E, 0]$	$[1, 0, 0, 63]$	$[FC, FC, 0, 9E]$	$[0, 1, 63, 0]$
$[0, 15, C7, C7]$	$[1, 0, 0, D3]$	$[15, 0, C7, C7]$	$[0, 1, D3, 0]$

Table 7: The sets of related differentials over M_3.

$\hat{\mathbf{b}}$	$\hat{\mathbf{c}}$	$\hat{\mathbf{b}'}$	$\hat{\mathbf{c}'}$
$[1, 0, 0, 50]$	$[E3, A1, ED, 0]$	$[1, 4, 54, 0]$	$[E3, 0, 0, 4C]$
$[1, 0, 0, ED]$	$[0, C, EF, 7D]$	$[0, 98, 99, ED]$	$[E3, 0, 0, 7D]$
$[0, 1, 50, 0]$	$[A1, E3, 0, ED]$	$[4, 1, 0, 54]$	$[0, E3, 4C, 0]$
$[0, 1, ED, 0]$	$[C, 0, 7D, EF]$	$[98, 0, ED, 99]$	$[0, E3, 7D, 0]$

Table 8: The sets of related differentials over M_4.

$\hat{\mathbf{b}}$	$\hat{\mathbf{c}}$	$\hat{\mathbf{b}'}$	$\hat{\mathbf{c}'}$
$[1, 0, 0, 0]$	$[F, DF, D0, 75]$	$[1, 58, A1, F9]$	$[0, 0, 0, 75]$
$[0, 1, 0, 0]$	$[DF, F, 75, D0]$	$[58, 1, F9, A1]$	$[0, 0, 75, 0]$
$[0, 0, 1, 0]$	$[D0, 75, F, DF]$	$[A1, F9, 1, 58]$	$[0, 75, 0, 0]$
$[0, 0, 0, 1]$	$[75, D0, DF, F]$	$[F9, A1, 58, 1]$	$[75, 0, 0, 0]$

Table 9: The total number of related differentials and the relations between matrix elements

Matrix	Total number of related differentials	Relations between elements
M_1	1020	$ad + bc = c^2 + d^2 = 45$
M_2	2040	$ab + cd = a^2 + d^2 = B0$ $ac + bd = c^2 + d^2 = DB$
M_3	1020	$a(a + b + c + d) = a^2 + d^2 = FD$
M_4	1020	$a + b + c = 0$

B Some Resistant MDS Hadamard matrices in $\mathbb{F}_{2^8}^{4\times 4}$, $\mathbb{F}_{2^6}^{4\times 4}$ and $\mathbb{F}_{2^5}^{4\times 4}$

Table 10: First 100 resistant MDS matrices in $\mathbb{F}_{2^8}^{4\times 4}$ that satisfy no relation from $\mathbf{R}$ in Theorem 3, ensuring no related differentials. Matrix elements are in decimal.

[1 2 4 9]	[1 2 4 10]	[1 2 4 11]	[1 2 4 12]	[1 2 4 14]	[1 2 4 15]	[1 2 4 16]	[1 2 4 17]	[1 2 4 18]	[1 2 4 19]
[1 2 4 20]	[1 2 4 21]	[1 2 4 23]	[1 2 4 24]	[1 2 4 26]	[1 2 4 27]	[1 2 4 28]	[1 2 4 29]	[1 2 4 30]	[1 2 4 31]
[1 2 4 32]	[1 2 4 33]	[1 2 4 34]	[1 2 4 35]	[1 2 4 36]	[1 2 4 37]	[1 2 4 38]	[1 2 4 39]	[1 2 4 40]	[1 2 4 41]
[1 2 4 42]	[1 2 4 43]	[1 2 4 44]	[1 2 4 45]	[1 2 4 46]	[1 2 4 47]	[1 2 4 48]	[1 2 4 50]	[1 2 4 52]	[1 2 4 53]
[1 2 4 54]	[1 2 4 55]	[1 2 4 56]	[1 2 4 57]	[1 2 4 58]	[1 2 4 59]	[1 2 4 60]	[1 2 4 61]	[1 2 4 62]	[1 2 4 63]
[1 2 4 64]	[1 2 4 65]	[1 2 4 67]	[1 2 4 68]	[1 2 4 69]	[1 2 4 70]	[1 2 4 71]	[1 2 4 72]	[1 2 4 73]	[1 2 4 74]
[1 2 4 75]	[1 2 4 76]	[1 2 4 77]	[1 2 4 78]	[1 2 4 79]	[1 2 4 80]	[1 2 4 81]	[1 2 4 82]	[1 2 4 83]	[1 2 4 84]
[1 2 4 85]	[1 2 4 86]	[1 2 4 87]	[1 2 4 88]	[1 2 4 89]	[1 2 4 90]	[1 2 4 91]	[1 2 4 92]	[1 2 4 93]	[1 2 4 94]
[1 2 4 95]	[1 2 4 96]	[1 2 4 97]	[1 2 4 98]	[1 2 4 99]	[1 2 4 100]	[1 2 4 101]	[1 2 4 102]	[1 2 4 103]	[1 2 4 104]
[1 2 4 106]	[1 2 4 107]	[1 2 4 108]	[1 2 4 109]	[1 2 4 110]	[1 2 4 111]	[1 2 4 112]	[1 2 4 113]	[1 2 4 114]	[1 2 4 115]

Table 11: First 100 resistant MDS matrices in $\mathbb{F}_{2^6}^{4\times 4}$ which do not satisfy any relation from the set $\mathbf{R}$.

[1 2 4 9]	[1 2 4 10]	[1 2 4 11]	[1 2 4 12]	[1 2 4 14]	[1 2 4 15]	[1 2 4 16]	[1 2 4 17]	[1 2 4 21]	[1 2 4 24]
[1 2 4 26]	[1 2 4 27]	[1 2 4 28]	[1 2 4 30]	[1 2 4 31]	[1 2 4 32]	[1 2 4 34]	[1 2 4 35]	[1 2 4 37]	[1 2 4 38]
[1 2 4 39]	[1 2 4 40]	[1 2 4 41]	[1 2 4 42]	[1 2 4 43]	[1 2 4 45]	[1 2 4 46]	[1 2 4 47]	[1 2 4 51]	[1 2 4 55]
[1 2 4 56]	[1 2 4 57]	[1 2 4 58]	[1 2 4 59]	[1 2 4 61]	[1 2 4 63]	[1 2 5 9]	[1 2 5 11]	[1 2 5 12]	[1 2 5 14]
[1 2 5 16]	[1 2 5 17]	[1 2 5 18]	[1 2 5 19]	[1 2 5 20]	[1 2 5 24]	[1 2 5 25]	[1 2 5 27]	[1 2 5 28]	[1 2 5 29]
[1 2 5 30]	[1 2 5 32]	[1 2 5 33]	[1 2 5 34]	[1 2 5 36]	[1 2 5 39]	[1 2 5 42]	[1 2 5 43]	[1 2 5 44]	[1 2 5 46]
[1 2 5 47]	[1 2 5 48]	[1 2 5 49]	[1 2 5 50]	[1 2 5 52]	[1 2 5 61]	[1 2 6 8]	[1 2 6 10]	[1 2 6 14]	[1 2 6 15]
[1 2 6 17]	[1 2 6 18]	[1 2 6 19]	[1 2 6 22]	[1 2 6 23]	[1 2 6 24]	[1 2 6 26]	[1 2 6 27]	[1 2 6 29]	[1 2 6 30]
[1 2 6 31]	[1 2 6 33]	[1 2 6 34]	[1 2 6 35]	[1 2 6 41]	[1 2 6 44]	[1 2 6 45]	[1 2 6 47]	[1 2 6 48]	[1 2 6 49]
[1 2 6 50]	[1 2 6 51]	[1 2 6 55]	[1 2 6 56]	[1 2 6 57]	[1 2 6 58]	[1 2 6 59]	[1 2 6 61]	[1 2 6 63]	[1 2 7 8]

Table 12: First 100 resistant MDS matrices in $\mathbb{F}_{2^5}^{4\times 4}$ which do not satisfy any relation from the set $\mathbf{R}$.

[1 2 4 9]	[1 2 4 16]	[1 2 4 17]	[1 2 4 19]	[1 2 4 20]	[1 2 4 24]	[1 2 4 26]	[1 2 4 27]	[1 2 4 29]	[1 2 5 13]
[1 2 5 17]	[1 2 5 23]	[1 2 5 27]	[1 2 5 28]	[1 2 5 31]	[1 2 6 8]	[1 2 6 14]	[1 2 6 15]	[1 2 6 17]	[1 2 6 27]
[1 2 6 29]	[1 2 6 31]	[1 2 7 8]	[1 2 7 13]	[1 2 7 21]	[1 2 7 23]	[1 2 7 29]	[1 2 7 31]	[1 2 8 6]	[1 2 8 7]
[1 2 8 13]	[1 2 8 15]	[1 2 8 18]	[1 2 8 25]	[1 2 8 28]	[1 2 9 4]	[1 2 9 21]	[1 2 10 18]	[1 2 10 24]	[1 2 10 28]
[1 2 10 30]	[1 2 10 31]	[1 2 11 14]	[1 2 11 15]	[1 2 11 16]	[1 2 11 25]	[1 2 11 29]	[1 2 12 16]	[1 2 12 18]	[1 2 12 21]
[1 2 12 23]	[1 2 12 25]	[1 2 12 26]	[1 2 12 27]	[1 2 12 28]	[1 2 13 5]	[1 2 13 7]	[1 2 13 8]	[1 2 13 17]	[1 2 13 18]
[1 2 13 21]	[1 2 13 25]	[1 2 13 27]	[1 2 14 6]	[1 2 14 11]	[1 2 14 16]	[1 2 14 17]	[1 2 14 19]	[1 2 14 21]	[1 2 14 30]
[1 2 14 31]	[1 2 15 6]	[1 2 15 8]	[1 2 15 11]	[1 2 15 17]	[1 2 15 25]	[1 2 15 29]	[1 2 16 4]	[1 2 16 11]	[1 2 16 12]
[1 2 16 14]	[1 2 16 20]	[1 2 16 23]	[1 2 16 26]	[1 2 16 28]	[1 2 17 4]	[1 2 17 5]	[1 2 17 6]	[1 2 17 13]	[1 2 17 14]
[1 2 17 15]	[1 2 18 8]	[1 2 18 10]	[1 2 18 12]	[1 2 18 13]	[1 2 18 22]	[1 2 18 26]	[1 2 18 27]	[1 2 18 28]	[1 2 18 31]

Table 13: Some lightweight matrices in $\mathcal{M}_1$ alongside their inverses and respective XOR costs. Values are represented in decimal.

Matrices	**Cost**	**Inverse Matrices**	**Cost**
1 2 4 9	120	76 152 43 26	140
1 2 4 11	120	237 193 153 5	140
1 2 4 16	120	229 209 185 210	144
1 2 4 18	120	41 82 164 244	136
1 2 4 19	120	192 155 45 239	136
1 2 4 20	120	238 199 149 247	140
1 2 4 24	120	233 201 137 27	128
1 2 4 27	120	19 38 76 134	140
1 2 4 28	120	97 194 159 240	136
1 2 4 29	120	23 46 92 152	136
1 2 4 30	120	34 68 136 209	140
1 2 4 31	120	240 251 237 190	144
1 2 4 34	120	250 239 197 157	132
1 2 4 37	120	244 243 253 160	140
1 2 4 39	120	51 102 204 163	140
1 2 4 40	120	53 106 212 73	140
1 2 4 42	120	187 109 218 72	140
1 2 4 44	120	10 20 40 35	136
1 2 4 48	120	175 69 138 34	136
1 2 4 50	120	54 108 216 187	144

Table 14: Cost analysis of some matrices using methods of [XZL+20]

Matrix	**Cost**
1 2 4 9	131
1 2 4 11	140
1 2 4 16	119
1 2 4 18	122
1 2 4 19	136

C Impossible Matrix Spaces

Based on our results and experiments discussed in the Sections 3,4 and 5, we summarize the Hadamard matrix spaces where all the matrices admit related differentials in the Table 15 given below.

Table 15: Hadamard matrix spaces with no resistant matrices

Matrix Space	Resistant Matrices	Reference
$\mathbb{F}_{2^3}^{4\times 4}$	None	Section 4.1
$\mathbb{F}_{2^4}^{4\times 4}$	None	Section 4.1
$\mathbb{F}_{2^4}^{8\times 8}$	None	Section 5
$\mathbb{F}_{2^5}^{8\times 8}$	None	Section 5

D Binary Matrix Representation of Multiplication by x in $\mathbb{F}_{2^8}$

For readers interested in doing lightweight analysis of the resistant matrices from their corresponding binary matrix form, in this section we provide brief example guide on how to form the corresponding binary matrix representing multiplication by an element in $\mathbb{F}_{2^8}$. We define $\mathbb{F}_{2^8}$ as

$$\mathbb{F}_{2^8} \cong \frac{\mathbb{F}_2[x]}{(x^8 + x^4 + x^3 + x + 1)}.$$

Each element $\alpha \in \mathbb{F}_{2^8}$ can be written as

$$\alpha(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

where $a_i \in \{0,1\}$. The field element $\boldsymbol{x}$ (which we also call “2”) acts by left-shifting these coefficients and reducing modulo the irreducible polynomial.

Step 1: Multiply by x.

$$x \cdot \alpha(x) = x\big(a_7x^7 + a_6x^6 + \cdots + a_1x + a_0\big) = a_7x^8 + a_6x^7 + \cdots + a_1x^2 + a_0x.$$

Step 2: Reduction. In $\mathbb{F}_{2^8}$, we have

$$x^8 \equiv x^4 + x^3 + x + 1 \pmod{x^8 + x^4 + x^3 + x + 1}.$$

Thus:

$$a_7 \cdot x^8 = a_7\left(x^4 + x^3 + x + 1\right).$$

Collecting like terms gives the coefficients

$$b_7 = a_6,\ b_6 = a_5,\ b_5 = a_4,\ b_4 = a_3 \oplus a_7,\ b_3 = a_2 \oplus a_7,\ b_2 = a_1,\ b_1 = a_0 \oplus a_7,\ b_0 = a_7.$$

Hence,

$$x \cdot \alpha(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0.$$

Step 3: Form the Matrix. We view α as the 8-bit column vector $\mathbf{a} = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)^T$. Its image under multiplication by x is $\mathbf{b} = (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0)^T$. From the relations above:

$$\begin{pmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}}_{M_x = M_2} \begin{pmatrix} a_7 \\ a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix}.$$

This 8×8 binary matrix M_2 (also denoted M_x) thus represents *multiplication by 2 (=x)* in $\mathbb{F}_{2^8}$.