On the Cryptographic Resilience of MDS Matrices

Kamil Otal[1], Ali Mert Sülçe[2], and Oğuz Yayla[2]

[1] TÜBİTAK BİLGEM National Research Institute of Electronics and Cryptology
Gebze, Kocaeli, Türkiye
kamil.otal@gmail.com
[2] Institute of Applied Mathematics, Middle East Technical University
Çankaya, Ankara, Türkiye
mert.sulce@metu.edu.tr; oguz@metu.edu.tr

Abstract. The zero-difference attack on AES, introduced by Bardeh and Rijmen in [ToSC 2022(2):43–62], exploits certain structural properties—referred to as related differentials—of the AES MDS matrix. Daemen and Rijmen had earlier shown that these related differentials appear not only in the AES MixColumns matrix but in every 4×4 circulant MDS matrix [CCDS 2009(1):47–69]. In the same paper, they also exhibited a 4×4 Hadamard MDS matrix for which no related differentials exist. Combining the two results, one can say, for instance, that some 4×4 Hadamard MDS matrices are more "secure" than any 4×4 circulant MDS matrix. Recently, Jha et al. investigated whether it is possible to characterize the 4×4 Hadamard MDS matrices for which no related differentials exist [IACR Commun. Cryptol. 2(1):37 (2025)]. As a result, they gave a systematic method to construct such "secure" matrices in terms of their parameters.

In this paper, we study the same problem for all 2×2 and 3×3 MDS matrices, in order to understand the cryptographic resilience of MDS matrices both theoretically and practically. We obtain the following:

- There are no related differentials for any 2×2 MDS matrices.
- There exist related differentials for all 3×3 circulant MDS matrices.
- There exist related differentials for all 3×3 involutory MDS matrices when the finite field has even size.
- We characterize all 3×3 MDS matrices for which there exist no related differentials when the size of the finite field is even.

In this way, we fill a gap for the cryptographic resilience problem of MDS matrices over finite fields.

These results provide a deeper understanding of the structural cryptographic resilience of small-dimensional MDS matrices and offer practical guidance for secure block cipher design.

MSC 2020: 94A60, 11T71.

Keywords: Maximum distance separable (MDS) matrices · Related differentials · Zero-difference attack

1 Introduction

The Advanced Encryption Standard (AES) [AES01] has been used and analyzed extensively worldwide since its standardization. In the construction of a modern block cipher such as AES, two main principles are taken into account: confusion and diffusion. Confusion is generally provided by substitution boxes (S-boxes), which are special nonlinear mappings on a finite-dimensional vector space over a finite field $\mathbb{F}_q$ with q elements, whereas diffusion is often provided by a maximum distance separable (MDS) matrix, i.e. the redundancy (check) part of a generator matrix of an MDS code.

Specifically, if r-bit to r-bit S-boxes are used in a block cipher, then an MDS matrix over the finite field $\mathbb{F}_{2^r}$ (or over $\mathrm{GL}(r, \mathbb{F}_2)$ in general) is preferred for maximal diffusion; see the wide trail strategy in [AES01] for further details. Such a choice makes it easy to count active S-boxes across rounds, which is important for establishing the resistance of the cipher against differential [BS91] and linear [Mat94] cryptanalysis.

1.1 Related Work

Owing to this maximal branch number, MDS matrices occupy a special place in cryptography. In recent decades, many studies have examined the construction and implementation of efficient MDS matrices.

Beyond efficiency, there are also security analyses of MDS matrices. Daemen and Rijmen [DR09] introduced the notion of related differentials for MDS matrices and gave examples of MDS matrices with and without related differentials. Later, Ronjom et al. [RBH17] introduced zero-difference patterns, which are deterministic 4-round characteristics for AES, together with a new key-recovery attack on 5-round AES. Subsequently, Bardeh and Rijmen [BR22] gave a general formulation of the zero-difference property that allows combining the 4-round zero-difference property with related differentials; this yields a new 7-round related-differential characteristic and, as a result, the first key-recovery attack on 7-round AES-128 based on the zero-difference property.

Most recently, Jha et al. investigated whether it is possible to characterize the 4×4 Hadamard MDS matrices for which no related differentials exist [JLG25]. As a result, they gave a systematic method to construct such "secure" matrices in terms of their parameters.

Recently, Kumar et al. [KYS26] showed that there exist related differentials for non-MDS matrices. The authors also presented some further results for MDS matrices some of which are related to the previous version of this paper.

We emphasize that, among the various attack types, only two—meet-in-the-middle (see, e.g., [DS08,DKS10,DFJ13]) and impossible differential (see, e.g., [LDKK08,BLNS18,LP21])—had succeeded in breaking the longest round-reduced versions of AES (e.g., up to 7 rounds of AES-128), until the 7-round attack on AES-128 of Bardeh and Rijmen [BR22].

1.2 Motivation

We remark that zero-difference attacks also appear to be applicable to most SPN ciphers in the literature. Note also that, in general, MDS matrices have been assumed to offer equivalent cryptographic resilience, so cryptographers have focused solely on their efficiency when choosing them. Examining MDS matrices from a security perspective is a recent and still rare effort, but one that seems likely to intensify.

Investigating such "secure" MDS matrices for the 4×4 case is a meaningful first step, since this is the most widely used dimension. However, 3×3, 8×8, 16×16, 24×24, and 32×32 MDS matrices are also used in cryptography (see, for example, [G+21,BNN+10,SLS+23,AMPŠ24]). Studying these other dimensions is therefore of interest, for both theoretical and practical reasons.

1.3 Our Contribution

In this paper, we investigate the existence of related differentials for 2×2 and 3×3 MDS matrices. Our main results are the following.

- There are no related differentials for any 2×2 MDS matrices.
- There exist related differentials for all 3×3 circulant MDS matrices.
- There exist related differentials for all 3×3 involutory MDS matrices when the finite field has even size.
- We characterize all 3×3 MDS matrices for which there exist no related differentials when the size of the finite field is even.

We emphasize that an arbitrary 3×3 matrix has nine independent entries, whereas a 4×4 Hadamard (or circulant) matrix has only four. This makes the investigation of all 3×3 MDS matrices harder at first sight. We therefore apply a suitable equivalence that reduces the number of independent entries to four, which makes the characterization of all 3×3 matrices tractable.

1.4 Organization of the Paper

The following section presents some preliminary material to make the paper as self-contained as possible. In Section 3 we prove that there are no related differentials for any 2×2 MDS matrix. Section 4 contains the proof of the existence of related differentials for all 3×3 circulant MDS matrices. The analogous result for all 3×3 involutory MDS matrices over finite fields of even size is given in Section 5. Section 6 is devoted to the characterization of all 3×3 MDS matrices over finite fields of even size in terms of the existence of related differentials. Finally, Section 7 concludes the paper and presents some questions as possible future work.

2 Preliminaries

This section presents some preliminary information in two subsections: MDS matrices and related differentials.

2.1 MDS Matrices

In this section, we briefly recall the fundamental notions of MDS matrices, mostly coming from coding theory.

Let $\mathbb{F}_q^n$ denote the set of vectors of length n with entries from the finite field $\mathbb{F}_q$ of size q. The function $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{R}$ given by $d(u, v) := |\{i : i \in \{1, 2, \ldots, n\},\ u_i \neq v_i\}|$ satisfies the metric axioms and is called the *Hamming distance*. A subset C of $\mathbb{F}_q^n$ endowed with the Hamming metric is called a *code*. The *minimum (Hamming) distance* of a code C is defined by $d(C) := \min\{d(u, v) : u, v \in C,\ u \neq v\}$. It satisfies the upper bound $d(C) \leq n + 1 - \log_q(|C|)$, known as the *Singleton bound*. A code that attains this bound with equality, i.e. $d(C) = n + 1 - \log_q(|C|)$, is called an *MDS code*.

The main parameters of a code C in $\mathbb{F}_q^n$ are denoted by $(n, |C|, d(C))_q$. In particular, if C is a k-dimensional subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q$, then we denote its main parameters by $[n, k, d(C)]_q$. MDS codes exist for many, but not all, parameter sets. In particular, the *MDS Conjecture* stated below characterizes the parameters for which linear MDS codes exist (see also [Rot06, Conjecture 11.16], for example).

Conjecture 1 (The MDS Conjecture). The parameters of a linear MDS code $[n, k, n - k + 1]_q$ of length n and dimension $k > 1$ over $\mathbb{F}_q$ satisfy the following.

$$n \leq \begin{cases} q + 1 & \text{if } k \in \{2\} \cup \{4, 5, \ldots, q - 2\}, \\ q + 1 & \text{if } k \in \{3, q - 1\} \text{ and } q \text{ is odd}, \\ q + 2 & \text{if } k \in \{3, q - 1\} \text{ and } q \text{ is even}, \\ k + 1 & \text{if } k \geq q. \end{cases}$$

A linear code is the row space of a $k \times n$ matrix over $\mathbb{F}_q$; such a matrix is called a *generator matrix* of the code. In particular, in systematic form a linear MDS code is represented by a $k \times n$ matrix $[I \mid M]$, the concatenation of the $k \times k$ identity matrix I and a $k \times (n - k)$ matrix M over $\mathbb{F}_q$. Here the redundancy (check) part M is called an *MDS matrix*. The minimum-distance property of a linear MDS code translates into the following well-known property of the corresponding MDS matrix.

Proposition 1. *Let u be a nonzero $k \times 1$ vector and M a $k \times k$ MDS matrix over $\mathbb{F}_q$. Then u and Mu together have at least $k + 1$ nonzero entries.*

Another important and characterizing feature of MDS matrices is the following algebraic property.

Proposition 2. *Let M be a $k \times k$ matrix over $\mathbb{F}_q$. Then M is MDS if and only if every square submatrix of M is nonsingular.*

The construction of MDS matrices is an important and intensively studied topic in mathematics and cryptography. We refer the reader to the recent comprehensive surveys [GPR+19,Leu23].

2.2 Related Differentials

Daemen and Rijmen [DR09] introduced a new type of difference, called a *related difference*, and studied the propagation of such differences through the AES linear layer. They also defined *related differentials*, which are pairs of related differences linked by a matrix. We use a slightly extended version of their definition, as follows.

Definition 1. *[DR09] Let M be an $n \times n$ matrix over $\mathbb{F}_q$. Then, the pair of n-dimensional vectors $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ over $\mathbb{F}_q$ is called a related differential if*

$$x_i y_i (x_i - y_i) = 0 \quad \text{and} \quad (Mx)_i (My)_i ((Mx)_i - (My)_i) = 0$$

for all $i \in \{0, 1, \ldots, n-1\}$.

We note that, originally, the four-tuple (x, y, Mx, My) was called a related differential in [BR22]. For brevity, we instead write $(x, y)_M$, or simply (x, y) when M is clear from the context.

3 Existence of Related Differentials for 2×2 MDS Matrices

The following theorem solves the problem completely for all 2×2 MDS matrices over any finite fields.

Theorem 1. *There are no related differentials for any 2×2 MDS matrices.*

Proof. Let M be a 2×2 MDS matrix over $\mathbb{F}_q$. Then

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

for some nonzero elements a, b, c, d in $\mathbb{F}_q$ with $ad - bc \neq 0$ (i.e. $\det M \neq 0$). Up to symmetry, there are only two types of candidate related differentials,

$$x = \begin{pmatrix} x_0 \\ 0 \end{pmatrix} \text{ and } y = \begin{pmatrix} 0 \\ y_1 \end{pmatrix}, \quad \text{and} \quad x = \begin{pmatrix} x_0 \\ 0 \end{pmatrix} \text{ and } y = \begin{pmatrix} x_0 \\ y_1 \end{pmatrix},$$

where x_0 and y_1 are nonzero elements of $\mathbb{F}_q$.

– In the first case, we have

$$Mx = \begin{pmatrix} ax_0 \\ cx_0 \end{pmatrix} \text{ and } My = \begin{pmatrix} by_1 \\ dy_1 \end{pmatrix}.$$

All entries of Mx and My are nonzero, so (Mx, My) can be a related difference only if $Mx = My$. Since $x \neq y$, this forces $\det M = 0$, a contradiction.

– In the second case, we have

$$Mx = \begin{pmatrix} ax_0 \\ cx_0 \end{pmatrix} \text{ and } My = \begin{pmatrix} ax_0 + by_1 \\ cx_0 + dy_1 \end{pmatrix}.$$

All entries of Mx are nonzero, so for (Mx, My) to be a related difference we need, in each coordinate, either $(My)_i = 0$ or $(My)_i = (Mx)_i$. If $(My)_0 = (My)_1 = 0$, then $My = 0$, contradicting the invertibility of M. Otherwise $(Mx)_0 = (My)_0$ or $(Mx)_1 = (My)_1$ holds, giving $by_1 = 0$ or $dy_1 = 0$, respectively, which again contradicts $b, d, y_1 \neq 0$.

As a result, we deduce that Mx and My cannot constitute a related differential. □

4 Existence of Related Differentials for 3×3 Circulant MDS Matrices

One of the most popular types of MDS matrix in the literature is the circulant MDS matrix. In this section, we show that every such 3×3 matrix has related differentials, as stated in the following theorem.

Theorem 2. *There exist related differentials for all* 3×3 *circulant MDS matrices.*

Proof. Let M be a 3×3 circulant MDS matrix over $\mathbb{F}_q$. Then

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

for some nonzero elements a, b, c in $\mathbb{F}_q$ such that every square submatrix of M is nonsingular. Consider the pair

$$x = \begin{pmatrix} x_0 \\ -ab^{-1}x_0 \\ 0 \end{pmatrix} \text{ and } y = \begin{pmatrix} 0 \\ -ab^{-1}x_0 \\ cb^{-1}x_0 \end{pmatrix}$$

for some nonzero $x_0 \in \mathbb{F}_q$. Then we have

$$Mx = \begin{pmatrix} 0 \\ (c - a^2b^{-1})x_0 \\ (b - acb^{-1})x_0 \end{pmatrix} \text{ and } My = \begin{pmatrix} (c^2b^{-1} - a)x_0 \\ (c - a^2b^{-1})x_0 \\ 0 \end{pmatrix}.$$

The pair (x, y) is a related difference at the input (the first and third coordinates have a zero, and the second coordinates coincide), and likewise Mx and My form a related difference at the output (the first entry of Mx and the third entry of My are zero, and their second entries coincide). Hence (x, y) is a related differential. □

Remark 1. Among the many types of pair (x, y) that could satisfy the related differential property, i.e. among

$$\begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 \\ y_1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 \\ y_1 \\ y_2 \end{pmatrix}, \quad \begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} x_0 \\ y_1 \\ 0 \end{pmatrix}, \ldots$$

the form best suited to the proof of Theorem 2 is, according to our computations,

$$\begin{pmatrix} x_0 \\ x_1 \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 \\ x_1 \\ y_2 \end{pmatrix}.$$

For the other types, either no related differential exists, or one needs algebraic relations among a, b, c, some of which contradict the MDS property of M. In other words, the density of related differentials among all possibilities is very low.

Remark 2. It is not surprising that there exist related differentials for all 3×3 circulant MDS matrices. Recall that related differentials also exist for all 4×4 circulant MDS matrices, as shown in [DR09].

5 Existence of Related Differentials for 3×3 Involutory MDS Matrices over Finite Fields of Even Size

Involutory MDS matrices, whose square is the identity matrix, form a special class of MDS matrices. When the inverse of the MDS matrix must also be implemented (for decryption, for example), involutory MDS matrices are preferable, since the matrix and its inverse coincide and therefore share the same implementation and efficiency. Güzel et al. [GSA+19] gave the following characterization of 3×3 involutory MDS matrices over finite fields of even size.

Proposition 3. *[GSA+19] Every 3×3 involutory MDS matrix over $\mathbb{F}_{2^r}$ has the form*

$$\begin{pmatrix} a_1 & (a_1+1)b_0 & (a_1+1)b_1 \\ (a_2+1)b_0^{-1} & a_2 & (a_2+1)b_0^{-1}b_1 \\ (a_1+a_2)b_1^{-1} & (a_1+a_2)b_1^{-1}b_0 & a_1+a_2+1 \end{pmatrix} \tag{1}$$

for some nonzero $a_1, a_2, b_0, b_1 \in \mathbb{F}_{2^r}$ satisfying $a_1 \neq a_2$, $a_1 + a_2 \neq 1$, $a_1 \neq 1$, and $a_2 \neq 1$.

We now use the representation in Proposition 3 to prove the following theorem, the main result of this section.

Theorem 3. *There exist related differentials for all 3×3 involutory MDS matrices when the finite field has even size.*

Proof. Let M be an involutory MDS matrix in the form of Equation (1). Take

$$x = \begin{pmatrix} x_0 \\ b_0^{-1}x_0 \\ 0 \end{pmatrix} \text{ and } y = \begin{pmatrix} 0 \\ b_0^{-1}x_0 \\ b_1^{-1}x_0 \end{pmatrix}$$

for some nonzero $x_0 \in \mathbb{F}_{2^r}$. Then $Mx = x$ and $My = y$, that is,

$$Mx = \begin{pmatrix} x_0 \\ b_0^{-1}x_0 \\ 0 \end{pmatrix} \text{ and } My = \begin{pmatrix} 0 \\ b_0^{-1}x_0 \\ b_1^{-1}x_0 \end{pmatrix}.$$

The pair (x, y) is a related difference at the input, and since $(Mx, My) = (x, y)$, it is also a related difference at the output. Hence (x, y) is a related differential. □

6 Characterization of All 3×3 MDS Matrices over Finite Fields of Even Size

In Sections 4 and 5 we obtained some negative results. We now search among all 3×3 MDS matrices for positive ones. To this end, the following reductions will be useful.

Theorem 4. *[KMS+24] Let M be an arbitrary square MDS matrix over a finite field $\mathbb{F}_q$. Then there exist square matrices D, N, E over $\mathbb{F}_q$ such that*

- *$M = DNE$,*
- *D and E are diagonal and invertible,*
- *N is unique, MDS, and its first row and first column contain only 1s.*

Proof. Direct computations yield the exact entries of D, N, and E in terms of the entries of M. Also note that multiplying a row (or column) by a nonzero scalar does not affect the nonzeroness of the determinant of a submatrix; therefore, the MDSness of M and N are the same. □

Example 1. We can illustrate Theorem 4 for 3×3 matrices as follows: Let

$$M = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix}.$$

Clearly, we have $m_i \neq 0$ for all $i \in \{1, 2, \ldots, 9\}$ since M is MDS. Then, we can take

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & m_4 m_1^{-1} & 0 \\ 0 & 0 & m_7 m_1^{-1} \end{pmatrix} \quad \text{and} \quad E = \begin{pmatrix} m_1 & 0 & 0 \\ 0 & m_2 & 0 \\ 0 & 0 & m_3 \end{pmatrix}.$$

Here, a different D and E pair can be preferred, but N does not change since it is unique.

Below, we present a reduction on the MDS matrix representation for finding related differentials by using Theorem 4.

Theorem 5. *Let M be a square MDS matrix and D, N, E are the corresponding decomposition of M as in Theorem 4 over a finite field $\mathbb{F}_q$. Then, there exists a related differential for M if and only if there exists one for N.*

Proof. The inverse of the diagonal matrix E preserves the zero/nonzero/equal pattern of the input pair (x, y). Likewise, the inverse of D preserves the same pattern of the output pair (Mx, My). □

Now we can use the reduced form in Theorem 5 to investigate all 3×3 MDS matrices over fields of even size.

Theorem 6. *Let M be a 3×3 MDS matrix over $\mathbb{F}_{2^r}$ and*

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

be its reduced form as described in Theorem 5 over $\mathbb{F}_{2^r}$. Then M has a related differential if and only if at least one of the following fifteen equations holds:

i) $a + d = 0$
ii) $b + c = 0$
iii) $ad + b = 0$,
iv) $ad + c = 0$,
v) $bc + a = 0$,
vi) $bc + d = 0$,
vii) $a + b + c + d = 0$,
viii) $ad + bc + a + b = 0$,
ix) $ad + bc + a + c = 0$,
x) $ad + bc + b + d = 0$,
xi) $ad + bc + c + d = 0$,
xii) $ad + a + b + d = 0$,
xiii) $ad + a + c + d = 0$,
xiv) $bc + a + b + c = 0$,
xv) $bc + b + c + d = 0$.

Before proving Theorem 6, we illustrate it with an infinite family of 3×3 MDS matrices for which no related differentials exist.

Example 2. Let $r > 8$ and α be a primitive normal element of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$. Let D and E be two arbitrary invertible diagonal 3×3 matrices over $\mathbb{F}_{2^r}$. Let

$$N = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^{2^2} & \alpha^{2^3} \end{pmatrix}.$$

Then DNE is an MDS matrix for which there exist no related differentials. It is clear that none of the 15 equations is valid for $a = \alpha$, $b = \alpha^2$, $c = \alpha^4$, and $d = \alpha^8$.

We now prove Theorem 6.

Proof. Since N is an MDS matrix (equivalently, M is MDS by Theorem 5), we have the conditions $ad + bc \neq 0$, $a \neq b$, $a \neq c$, $b \neq d$, $c \neq d$, $a, b, c, d \notin \{0, 1\}$, and $\det N = ad + bc + a + b + c + d \neq 0$. Let x and y be a related difference, and let $x' = Nx$ and $y' = Ny$ be the corresponding output pair. If x' and y' are also a related difference, we can conclude that N (and hence M) has a related differential.

We list all input differences that are related and check whether the corresponding output pairs are related differences or not.

Case 1: x and y each have one nonzero entry.

i) $x = \begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ y_1 \\ 0 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 \\ x_0 \\ x_0 \end{pmatrix}, y' = \begin{pmatrix} y_1 \\ ay_1 \\ cy_1 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_0 + y_1 \\ x_0 + ay_1 \\ x_0 + cy_1 \end{pmatrix}$.

Since all entries of x' and y' are nonzero, the output can be a related difference only if $x' = y'$, i.e. $x' \oplus y' = 0$. Therefore, $x_0 + y_1 = 0$, which means $x_0 = y_1$. Together with $x_0 + ay_1 = 0$ and $x_0 + cy_1 = 0$, this implies that a and c are 1, which is a contradiction. Thus, there are no related differentials in this case.

ii) $x = \begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ 0 \\ y_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 \\ x_0 \\ x_0 \end{pmatrix}, y' = \begin{pmatrix} y_2 \\ by_2 \\ dy_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_0 + y_2 \\ x_0 + by_2 \\ x_0 + dy_2 \end{pmatrix}$.

Because of very similar reasons to i, we get $b = 1$ and $d = 1$. So this is a contradiction.

iii) $x = \begin{pmatrix} 0 \\ x_1 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ 0 \\ y_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_1 \\ ax_1 \\ cx_1 \end{pmatrix}, y' = \begin{pmatrix} y_2 \\ by_2 \\ dy_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_1 + y_2 \\ ax_1 + by_2 \\ cx_1 + dy_2 \end{pmatrix}$.

Since all entries of x' and y' are nonzero, the output can be a related difference only if $x' \oplus y' = 0$. We then have $x_1 + y_2 = 0$, $ax_1 + by_2 = 0$, and $cx_1 + dy_2 = 0$, which give $a = b$ and $c = d$, contradictions.

Case 2: x has one and y has two nonzero entries.

i) $x = \begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} x_0 \\ y_1 \\ 0 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 \\ x_0 \\ x_0 \end{pmatrix}, y' = \begin{pmatrix} x_0 + y_1 \\ x_0 + ay_1 \\ x_0 + cy_1 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} y_1 \\ ay_1 \\ cy_1 \end{pmatrix}$.

This case is the same as Case 1-i.

ii) $x = \begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} x_0 \\ 0 \\ y_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 \\ x_0 \\ x_0 \end{pmatrix}, y' = \begin{pmatrix} x_0 + y_2 \\ x_0 + by_2 \\ x_0 + dy_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} y_2 \\ by_2 \\ dy_2 \end{pmatrix}$.

This case is the same as Case 1-ii.

iii) $x = \begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ y_1 \\ y_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 \\ x_0 \\ x_0 \end{pmatrix}, y' = \begin{pmatrix} y_1 + y_2 \\ ay_1 + by_2 \\ cy_1 + dy_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_0 + y_1 + y_2 \\ x_0 + ay_1 + by_2 \\ x_0 + cy_1 + dy_2 \end{pmatrix}$.

Since x_0, y_1 and y_2 are non-zero, we have two possibilities: $y_1 + y_2 = 0$; $x_0 + y_1 + y_2 = 0$.

Firstly, assume $y_1 + y_2 = 0$ which means $y_1 = y_2$. Then for the second entry, we have $ay_1 + by_2 = 0$ or $x_0 + ay_1 + by_2 = 0$. If $ay_1 + by_2 = 0 \rightarrow (a + b)y_1 = 0 \rightarrow a = b$, it is impossible. So $x_0 + ay_1 + by_2 = 0 \rightarrow x_0 + (a + b)y_1 = 0$. For the third entry, we have $cy_1 + dy_2 = 0$, which results in $c = d$, so it is a contradiction. Therefore, $x_0 + cy_1 + dy_2 = 0 \rightarrow (a + b)y_1 + cy_1 + dy_1 = 0$. Thus we get **a+b+c+d=0**.

Secondly, assume $x_0 + y_1 + y_2 = 0$. For the second entry, we have $ay_1 + by_2 = 0$ or $x_0 + ay_1 + by_2 = 0$. If $ay_1 + by_2 = 0 \rightarrow y_2 = \frac{a}{b}y_1$. In this case, for the third entry, again we have two options: $cy_1 + dy_2 = 0 \rightarrow cy_1 + \frac{ad}{b}y_1 = 0 \rightarrow ad + bc = 0$ which is a contradiction or $x_0 + cy_1 + dy_2 = 0 \rightarrow (c + 1)y_1 + (d + 1)y_2 = 0 \rightarrow (c + 1)y_1 + (d + 1)\frac{a}{b}y_1 = 0$. Thus we get **ad+bc+a+b=0**. On the other hand, if $x_0 + ay_1 + by_2 = 0 \rightarrow (a + 1)y_1 + (b + 1)y_2 = 0$. For the third entry, if $cy_1 + dy_2 = 0$, then $cy_1 + d\frac{a+1}{b+1}y_1 = 0$ so we get **ad+bc+c+d=0**. Lastly, if $x_0 + cy_1 + dy_2 = 0$, then $(c + 1)y_1 + (d + 1)y_2 = 0 \rightarrow (c + 1)y_1 + (d + 1)\frac{a+1}{b+1}y_1 = 0$. In this case, we get $ad + bc + a + b + c + d = 0$, which is impossible since $\det N = ad + bc + a + b + c + d \neq 0$.

iv) $x = \begin{pmatrix} 0 \\ x_1 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} y_0 \\ x_1 \\ 0 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_1 \\ ax_1 \\ cx_1 \end{pmatrix}, y' = \begin{pmatrix} x_1 + y_0 \\ ax_1 + y_0 \\ cx_1 + y_0 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} y_0 \\ y_0 \\ y_0 \end{pmatrix}$.

Here every entry of x' is nonzero while no entry of $x' \oplus y' = (y_0, y_0, y_0)$ vanishes, so the output can be a related difference only if $y' = 0$. We then have $x_1 + y_0 = 0$, $ax_1 + y_0 = 0$, $cx_1 + y_0 = 0$, which give $x_1 = y_0$ and hence $a = c = 1$, contradictions.

v) $x = \begin{pmatrix} 0 \\ x_1 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ x_1 \\ y_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_1 \\ ax_1 \\ cx_1 \end{pmatrix}, y' = \begin{pmatrix} x_1 + y_2 \\ ax_1 + by_2 \\ cx_1 + dy_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} y_2 \\ by_2 \\ dy_2 \end{pmatrix}$.

This is the same with Case 1-iii.

vi) $x = \begin{pmatrix} 0 \\ x_1 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} y_0 \\ 0 \\ y_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_1 \\ ax_1 \\ cx_1 \end{pmatrix}, y' = \begin{pmatrix} y_0 + y_2 \\ y_0 + by_2 \\ y_0 + dy_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_1 + y_0 + y_2 \\ ax_1 + y_0 + by_2 \\ cx_1 + y_0 + dy_2 \end{pmatrix}$.

Since all input values are non-zero, we have two possibilities: $y_0 + y_2 = 0$ or $x_1 + y_0 + y_2 = 0$.

Firstly, assume $y_0 + y_2 = 0 \rightarrow y_0 = y_2$. For the second entry $y_0 + by_2 = 0$ or $ax_1 + y_0 + by_2 = 0$. If $y_0 + by_2 = 0$, $(b+1)y_0 = 0 \rightarrow b = 1$ which is not possible. If $ax_1 + y_0 + by_2 = 0$, we get $ax_1 + (b+1)y_0 = 0 \rightarrow x_1 = \frac{b+1}{a} y_0$. For the third entry again $y_0 + dy_2 = 0 \rightarrow d = 1$ which results to contradiction and $cx_1 + y_0 + dy_2 = 0 \rightarrow cx_1 + (d+1)y_0 = 0 \rightarrow (c\frac{b+1}{a} + (d+1))y_0 = 0$ Therefore, we get **ad+bc+a+c=0**.

Secondly, assume $x_1 + y_0 + y_2 = 0$ for the first row and the second one, again we have two options. One of them is $y_0 + by_2 = 0 \rightarrow y_0 = by_2$. In this case for the third row, we have $y_0 + dy_2 = 0$ which is a contradiction because $(b+d)y_2 = 0 \rightarrow b = d$ or $cx_1 + y_0 + dy_2 = 0 \rightarrow cx_1 + (b+d)y_2 = 0 \rightarrow c(y_0 + y_2) + (b+d)y_2 = 0 \rightarrow bcy_2 + cy_2 + (b+d)y_2 = 0$. Thus, we get **bc+c+b+d=0**.

The other case for the second row is $ax_1 + y_0 + by_2 = 0 \rightarrow (a+1)x_1 + (b+1)y_2 = 0$. For the third row, one case is $y_0 + dy_2 = 0$ and the other is $cx_1 + y_0 + dy_2 = 0$. If $y_0 + dy_2 = 0 \rightarrow x_1 + (d+1)y_2 = (\frac{b+1}{a+1} + (d+1))y_2 = 0$. Thus, we get **ad+a+b+d=0**.

For the $cx_1 + y_0 + dy_2 = 0$, we have $(c+1)x_1 + (d+1)y_2 = 0 \rightarrow ((c+1)\frac{b+1}{a+1} + (d+1))y_2 = 0$. Thus, we get $ad + bc + a + b + c + d = 0$ which is a contradiction.

vii) $x = \begin{pmatrix} 0 \\ 0 \\ x_2 \end{pmatrix}$ and $y = \begin{pmatrix} y_0 \\ 0 \\ x_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_2 \\ bx_2 \\ dx_2 \end{pmatrix}, y' = \begin{pmatrix} y_0 + x_2 \\ y_0 + bx_2 \\ y_0 + dx_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} y_0 \\ y_0 \\ y_0 \end{pmatrix}$.

Here every entry of x' is nonzero, so the output can be a related difference only if $y' = 0$. Then $y_0 + x_2 = 0 \rightarrow y_0 = x_2$, which forces $b = 1$ and $d = 1$ in the other rows, a contradiction.

viii) $x = \begin{pmatrix} 0 \\ 0 \\ x_2 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ y_1 \\ x_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_2 \\ bx_2 \\ dx_2 \end{pmatrix}, y' = \begin{pmatrix} y_1 + x_2 \\ ay_1 + bx_2 \\ cy_1 + dx_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} y_1 \\ ay_1 \\ cy_1 \end{pmatrix}$.

Here every entry of x' is nonzero, so the output can be a related difference only if $y' = 0$. Then $y_1 + x_2 = 0 \rightarrow y_1 = x_2$, which forces $a = b$ and $c = d$ in the other rows, a contradiction.

ix) $x = \begin{pmatrix} 0 \\ 0 \\ x_2 \end{pmatrix}$ and $y = \begin{pmatrix} y_0 \\ y_1 \\ 0 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_2 \\ bx_2 \\ dx_2 \end{pmatrix}, y' = \begin{pmatrix} y_0 + y_1 \\ y_0 + ay_1 \\ y_0 + cy_1 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_2 + y_0 + y_1 \\ bx_2 + y_0 + ay_1 \\ dx_2 + y_0 + cy_1 \end{pmatrix}$.

For the first row, either $y_0 + y_1 = 0$ or $x_2 + y_0 + y_1 = 0$

If $y_0 + y_1 = 0$, we get $y_0 = y_1$. In the second row, either $y_0 + ay_1 = 0$ or $bx_2 + y_0 + ay_1 = 0$. If $y_0 + ay_1 = 0$, $y_0 + ay_0 = 0 \rightarrow a = 1$ which is a contradiction. So $bx_2 + y_0 + ay_1 = 0$ and we get $bx_2 + (a+1)y_0 = 0 \rightarrow x_2 = \frac{a+1}{b} y_0$. And for the last row, if $y_0 + cy_1 = 0$, again we get a contradiction because of $c = 1$. Therefore, $dx_2 + y_0 + cy_1 = 0$. In this case, $dx_2 + (c+1)y_0 = 0 \rightarrow (\frac{ad+d}{b} + c + 1)y_0 = 0$. Thus, we get **ad+bc+b+d=0**.

Now we study the other case for the first row: $x_2 + y_0 + y_1 = 0$. For the second row again, we have either $y_0 + ay_1 = 0$ or $bx_2 + y_0 + ay_1 = 0$. If $y_0 + ay_1 = 0$, then we can say $y_0 = ay_1$. For the third row, $y_0 + cy_1 = 0 \rightarrow (a + c)y_1 = 0 \rightarrow a = c$ we get contradiction. So the only way is $dx_2 + y_0 + cy_1 = 0$. Then $d(y_0 + y_1) + y_0 + cy_1 = 0 \rightarrow d(ay_1 + y_1) + (a + c)y_1 = 0 \rightarrow$ **ad+a+c+d=0**.

If the second row is $bx_2 + y_0 + ay_1 = 0$ we can say $(b+1)x_2 = (a+1)y_1$. For the third row, if $y_0 + cy_1 = 0 \rightarrow bx_2 + ay_1 + cy_1 = 0 \rightarrow (b\frac{a+1}{b+1} + a + c)y_1 = 0$. Therefore we get **bc+a+b+c=0**.

The last property is the third row $dx_2 + y_0 + cy_1 = 0$. Then $(d+1)x_2 + (c+1)y_1 = 0 \rightarrow (d+1)x_2 + (c+1)y_1 = 0 \rightarrow (d+1)\frac{a+1}{b+1}y_1 + (c+1)y_1 = 0$ Thus, we get $ad + bc + a + b + c + d = 0$ but it is not possible because $\det N \neq 0$.

Case 3: both x and y have two nonzero entries.

i) $x = \begin{pmatrix} x_0 \\ x_1 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} x_0 \\ 0 \\ y_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 + x_1 \\ x_0 + ax_1 \\ x_0 + cx_1 \end{pmatrix}, y' = \begin{pmatrix} x_0 + y_2 \\ x_0 + by_2 \\ x_0 + dy_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_1 + y_2 \\ ax_1 + by_2 \\ cx_1 + dy_2 \end{pmatrix}$.

Since this case is the same as the following one, we can skip this.

ii) $x = \begin{pmatrix} x_0 \\ x_1 \\ 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ x_1 \\ y_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 + x_1 \\ x_0 + ax_1 \\ x_0 + cx_1 \end{pmatrix}, y' = \begin{pmatrix} x_1 + y_2 \\ ax_1 + by_2 \\ cx_1 + dy_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_0 + y_2 \\ x_0 + by_2 \\ x_0 + dy_2 \end{pmatrix}$.

In this case, we have three options for the first row: $x_0 + x_1 = 0$, $x_1 + y_2 = 0$ or $x_0 + y_2 = 0$

If $x_0 + x_1 = 0 \to x_0 = x_1$, then for the second row again either $x_0 + ax_1 = 0$ or $ax_1 + by_2 = 0$ or $x_0 + by_2 = 0$. If $x_0 + ax_1 = 0 \to (a + 1)x_1 = 0 \to a = 1$ which is a contradiction. If $ax_1 + by_2 = 0$, then $x_1 = \frac{b}{a}y_2$. For the last row,$x_0 + cx_1 = 0$ means $c = 1$, again we get a contradiction. If $cx_1 + dy_2 = 0 \to c\frac{b}{a}y_2 + dy_2$, we get $bc + ad = 0$ which is a contradiction. So the only option for the last row is $x_0 + dy_2 = 0 \to x_1 + dy_2 = 0 \to \frac{b}{a}y_2 + dy_2$. Thus, we get **ad+b=0**. If the second is $x_0 + by_2 = 0$, we get a contradiction for the $x_0 + cx_1 = 0 \to c = 1$. If $cx_1 + dy_2 = 0 \to cx_0 + dy_2 = 0 \to cby_2 + dy_2 = 0$, we get **bc+d=0**. If $x_0 + dy_2 = 0 \to by_2 + dy_2 = 0$, we get the contradiction due to $b \neq d$.

If $x_1 + y_2 = 0 \to x_1 = y_2$, then again for the second row, either $x_0 + ax_1 = 0$ or $ax_1 + by_2 = 0$ or $x_0 + by_2 = 0$. If $x_0 + ax_1 = 0 \to x_0 = ax_1 = ay_2$. In this case, for the last row, $x_0 + cx_1 = 0 \to a = c$ and $cx_1 + dy_2 = 0 \to c = d$ result to contradictions. If $x_0 + dy_2 = 0 \to ay_2 + dy_2 = 0$, we get **a=d**. If $ax_1 + by_2 = 0 \to ax_1 + bx_1 = 0 \to a = b$, we get the contradiction. The last case for the second row is $x_0 + by_2 = 0$, which means $x_0 = bx_1 = by_2$. For the last row, in cases $cx_1 + dy_2 = 0 \to (c + d)y_2 = 0 \to c = d$ and $x_0 + dy_2 = 0 \to by_2 + dy_2 = 0 \to b = d$, we get contradictions. However, in $x_0 + cx_1 = 0 \to bx_1 + cx_1 = 0$, we get **b=c**.

If $x_0 + y_2 = 0 \to x_0 = y_2$, then again for the second row, either $x_0 + ax_1 = 0$ or $ax_1 + by_2 = 0$ or $x_0 + by_2 = 0$.The last one is impossible because in this case we get $b = 1$. If $x_0 + ax_1 = 0 \to x_0 = ax_1 = y_2$. For the last row, $x_0 + cx_1 = 0 \to a = c$ and $x_0 + dy_2 = 0 \to d = 1$ are contradictions. If $cx_1 + dy_2 = 0 \to cx_1 + dax_1 = 0$, we get **ad+c=0**. If $ax_1 + by_2 = 0 \to x_0 = \frac{a}{b}x_1 = y_2$. For the last row, $cx_1 + dy_2 = 0 \to cx_1 + d\frac{a}{b}x_1 = 0 \to ad + bc = 0$ and $x_0 + dy_2 = 0 \to d = 1$ are contradictions.If $x_0 + cx_1 = 0 \to \frac{a}{b}x_1 + cx_1 = 0$, we get **bc+a=0**.

iii) $x = \begin{pmatrix} x_0 \\ 0 \\ x_2 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ y_1 \\ x_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 + x_2 \\ x_0 + bx_2 \\ x_0 + dx_2 \end{pmatrix}, y' = \begin{pmatrix} x_2 + y_1 \\ ay_1 + bx_2 \\ cy_1 + dx_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_0 + y_1 \\ x_0 + ay_1 \\ x_0 + cy_1 \end{pmatrix}$.

In this case, we have three options for the first row: $x_0 + x_2 = 0$, $x_2 + y_1 = 0$ or $x_0 + y_1 = 0$

Firstly, we study $x_0 + x_2 = 0 \to x_0 = x_2$. For the second row, $x_0 + bx_2 =$

$x_2 + bx_2 = 0$ is the contradiction due to $b = 1$. If $ay_1 + bx_2 = 0 \rightarrow x_0 = x_2 = \frac{a}{b}y_1$, we get contradictions in cases $x_0 + dx_2 = 0 \rightarrow d = 1$ and $cy_1 + dx_2 = 0 \rightarrow cy_1 + d\frac{a}{b}y_1 = 0 \rightarrow ad + bc = 1$. Therefore, $x_0 + cy_1 = 0$ is the only possibility for the third row and we get $x_0 + cy_1 = 0 \rightarrow \frac{a}{b}y_1 + cy_1 = 0 \rightarrow$ **bc+a=0**. On the other hand, if $x_0 + ay_1 = 0 \rightarrow x_0 = x_2 = ay_1$, the only way for third row is $cy_1 + dx_2 = 0 \rightarrow cy_1 + day_1 = 0$ and we get **ad+c=0**.

Secondly, if $x_2 + y_1 = 0 \rightarrow x_2 = y_1$, $ay_1 + bx_2 = 0$ is contradiction due to $a \neq b$. If $x_0 + bx_2 = 0 \rightarrow x_0 = bx_2 = by_1$, $x_0 + dx_2 = 0 \rightarrow b = d$ and $cy_1 + dx_2 = 0 \rightarrow c = d$ are contradictions. Therefore, the only way for the last row is $x_0 + cy_1 = 0 \rightarrow by_1 + cy_1 = 0$ and we get **b=c**. Similarly, $cy_1 + dx_2 = 0$ and $x_0 + cy_1 = 0$ are impossible in case of $x_0 + ay_1 = 0$. In this case the only way is $x_0 + dx_2 = 0 \rightarrow ax_2 + dx_2 = 0$ and we get **a=d**.

Thirdly, if $x_0 + y_1 = 0 \rightarrow x_0 = y_1$, $x_0 + ay_1 = 0$ is contradiction due to $a \neq 1$. In case $x_0 + bx_2 = 0 \rightarrow x_0 = y_1 = bx_2$, if $x_0 + dx_2 = 0 \rightarrow bx_2 + dx_2 = 0 \rightarrow b = d$ and $x_0 + cy_1 = 0 \rightarrow x_0 + cx_0 = 0 \rightarrow c = 1$, we get contradictions. If $cy_1 + dx_2 = 0 \rightarrow cbx_2 + dx_2 = 0$, we get **bc+d=0**. On the other hand, if $ay_1 + bx_2 = 0 \rightarrow x_0 = y_1 = \frac{b}{a}x_2$, $cy_1 + dx_2 = 0 \rightarrow c\frac{b}{a}x_2 + dx_2 = 0 \rightarrow bc + ad = 0$ and $x_0 + cy_1 = 0 \rightarrow c = 1$ are contradictions but if $x_0 + dx_2 = 0 \rightarrow \frac{b}{a}x_2 + dx_2 = 0$, we get we get **ad+b=0**.

Case 4: x has three and y has one nonzero entry.

i) $x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$ and $y = \begin{pmatrix} x_0 \\ 0 \\ 0 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 + x_1 + x_2 \\ x_0 + ax_1 + bx_2 \\ x_0 + cx_1 + dx_2 \end{pmatrix}, y' = \begin{pmatrix} x_0 \\ x_0 \\ x_0 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_1 + x_2 \\ ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix}$.

For the first row, we have two options, either $x_0 + x_1 + x_2 = 0$ or $x_1 + x_2 = 0$

If $x_1 + x_2 = 0 \rightarrow x_1 = x_2$, we get a contradiction for case $ax_1 + bx_2 = 0 \rightarrow (a + b)x_1 = 0 \rightarrow a = b$. On the other hand, in the case $x_0 + ax_1 + bx_2 = 0 \rightarrow x_0 = (a + b)x_1$, we have only one option because $cx_1 + dx_2 = 0 \rightarrow c = d$ is a contradiction, so we have $x_0 + cx_1 + dx_2 = 0 \rightarrow x_0 + (c + d)x_1 = 0 \rightarrow (a + b + c + d)x_1 = 0$ and **a+b+c+d=0**.

Now let $x_0 + x_1 + x_2 = 0$. If $x_0 + ax_1 + bx_2 = 0 \rightarrow (a + 1)x_1 + (b + 1)x_2 = 0 \rightarrow x_2 = \frac{a+1}{b+1}x_1$. In this case, we have two options for the last row. Firstly, if $x_0 + cx_1 + dx_2 = 0 \rightarrow (c + 1)x_1 + (d + 1)x_2 = 0 \rightarrow ((c+1) + (d+1)\frac{a+1}{b+1})x_1 = 0$, we get $ad + bc + a + b + c + d = 0$ but this is a contradiction. Secondly, if $cx_1 + dx_2 = 0 \rightarrow cx_1 + d\frac{a+1}{b+1})x_1 = 0$, we get **ad+bc+c+d=0**.

In this case, if we assume $ax_1 + bx_2 = 0$ for the second row, we have only one option because $cx_1 + dx_2 = 0 \rightarrow cx_1 + d\frac{a}{b}x_1 = 0 \rightarrow ad + bc = 0$

is the contradiction. The possible case is $x_0+cx_1+dx_2=0$ and we get **ad+bc+a+b=0**.

ii) $x=\begin{pmatrix}x_0\\x_1\\x_2\end{pmatrix}$ and $y=\begin{pmatrix}0\\x_1\\0\end{pmatrix}$

So, $x'=\begin{pmatrix}x_0+x_1+x_2\\x_0+ax_1+bx_2\\x_0+cx_1+dx_2\end{pmatrix}, y'=\begin{pmatrix}x_1\\ax_1\\cx_1\end{pmatrix}$ and $x'\oplus y'=\begin{pmatrix}x_0+x_2\\x_0+bx_2\\x_0+dx_2\end{pmatrix}$.

For the first row, we have two options, either $x_0+x_2=0$ or $x_0+x_1+x_2=0$.

Let $x_0+x_2=0\rightarrow x_0=x_2$. For $x'\oplus y'$, we get the contradiction in the second and third row. Therefore, the second row can be $x_0+ax_1+bx_2=0\rightarrow x_1=\frac{b+1}{a}x_0$. For the third row, $x_0+cx_1+dx_2=0$. Then $(b+1)x_0+cx_1=0\rightarrow(d+1)x_0+c\frac{b+1}{a}x_0=0$. Thus, we get **ad+bc+a+c=0**.

Now let $x_0+x_1+x_2=0$. If $x_0+ax_1+bx_2=0\rightarrow(a+1)x_1+(b+1)x_2=0$, we have two different cases for the last row. The first is $x_0+cx_1+dx_2=0$. In this case, $(c+1)x_1+(d+1)x_2=0\rightarrow(c+1)x_1+(d+1)\frac{a+1}{b+1}x_1=0$ and we get $ad+bc+a+b+c+d=0$ but $\det N\neq 0$, contradiction. The second is $x_0+dx_2=0\rightarrow x_1+(d+1)x_2=0\rightarrow\frac{b+1}{a+1}x_2+(d+1)x_2=0$, we get **ad+a+b+d=0**. If we change the case for the second row that is $x_0+bx_2=0\rightarrow x_0=bx_2$, we get the contradiction in case $x_0+dx_2=bx_2+dx_2=0\rightarrow b=d$ but in case $x_0+cx_1+dx_2=x_0+c(x_0+x_2)+dx_2=(c+1)bx_2+(c+d)x_2$, we get **bc+b+c+d=0**.

iii) $x=\begin{pmatrix}x_0\\x_1\\x_2\end{pmatrix}$ and $y=\begin{pmatrix}0\\0\\x_2\end{pmatrix}$

So, $x'=\begin{pmatrix}x_0+x_1+x_2\\x_0+ax_1+bx_2\\x_0+cx_1+dx_2\end{pmatrix}, y'=\begin{pmatrix}x_2\\bx_2\\dx_2\end{pmatrix}$ and $x'\oplus y'=\begin{pmatrix}x_0+x_1\\x_0+ax_1\\x_0+cx_1\end{pmatrix}$.

For the first row, we have two options, either $x_0+x_1=0$ or $x_0+x_1+x_2=0$.

Similar to the previous cases, we get **ad+bc+b+d=0** if $x_0+x_1=0$, $x_0+ax_1+bx_2$ and $x_0+cx_1+dx_2$. We get some contradictions in other cases when $x_0+x_1=0$.

On the other hand, if $x_0+x_1+x_2$, we get $ad+bc+a+b+c+d=0$ in case $x_0+ax_1+bx_2=0$ and $x_0+cx_1+dx_2=0$ but this is not possible because $\det N\neq 0$. We get **bc+a+b+c=0** in case $x_0+ax_1+bx_2=0$ and $x_0+cx_1=0$. Lastly, we get **ad+a+c+d=0** in case $x_0+ax_1=0$ and $x_0+cx_1+dx_2=0$.

Case 5: x has three and y has two nonzero entries.

i) $x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$ and $y = \begin{pmatrix} x_0 \\ x_1 \\ 0 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 + x_1 + x_2 \\ x_0 + ax_1 + bx_2 \\ x_0 + cx_1 + dx_2 \end{pmatrix}, y' = \begin{pmatrix} x_0 + x_1 \\ x_0 + ax_1 \\ x_0 + cx_1 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_2 \\ bx_2 \\ dx_2 \end{pmatrix}$.

This is the same case with 4-iii.

ii) $x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$ and $y = \begin{pmatrix} x_0 \\ 0 \\ x_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 + x_1 + x_2 \\ x_0 + ax_1 + bx_2 \\ x_0 + cx_1 + dx_2 \end{pmatrix}, y' = \begin{pmatrix} x_0 + x_2 \\ x_0 + bx_2 \\ x_0 + dx_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_1 \\ ax_1 \\ cx_1 \end{pmatrix}$.

This is the same case as 4-ii.

iii) $x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$ and $y = \begin{pmatrix} 0 \\ x_1 \\ x_2 \end{pmatrix}$

So, $x' = \begin{pmatrix} x_0 + x_1 + x_2 \\ x_0 + ax_1 + bx_2 \\ x_0 + cx_1 + dx_2 \end{pmatrix}, y' = \begin{pmatrix} x_1 + x_2 \\ ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix}$ and $x' \oplus y' = \begin{pmatrix} x_0 \\ x_0 \\ x_0 \end{pmatrix}$.

This is the same case with 4-i.

□

Remark 3. In the previous version of this paper, Theorem 6 was written with a small typo even if its proof was complete. Particularly, we missed two equations among 15, but now the current version is complete. We thank the authors of [KYS26] for bringing this point to our attention.

7 Conclusion and Future Work

In this paper, we proved the existence and nonexistence of related differentials for MDS matrices over finite fields in several cases, in particular:

- There are no related differentials for any 2×2 MDS matrices.
- There exist related differentials for all 3×3 circulant MDS matrices.
- There exist related differentials for all 3×3 involutory MDS matrices when the finite field has even size.
- We characterize all 3×3 MDS matrices for which there exist no related differentials when the finite field has even size.

In this way, we explicitly identify, in various cases, which types of MDS matrices have more or less cryptographic resilience.

Our results can be extended in several directions, as a number of natural questions arise within this scope, for example:

1. For 4×4 MDS matrices, answers are known so far for circulant and Hadamard matrices. What can be said for other types of 4×4 MDS matrices, particularly generalized Hadamard, Cauchy, and involutory matrices?

2. What happens for $n \times n$ MDS matrices when $n \geq 5$? (Partially addressed for circulant matrices in [KYS26].)
3. The number and types of related differentials are also of interest, since some related differentials may be easier to exploit than others in zero-difference attacks. (Partially addressed for circulant matrices in [KYS26].)

References

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

[AMPŠ24] Tomer Ashur, Mohammad Mahzoun, Jim Posen, and Danilo Šijačić. Vision mark-32: Zk-friendly hash function over binary tower fields. *Cryptology ePrint Archive*, 2024.

[BLNS18] Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder. Making the impossible possible. *Journal of Cryptology*, 31(1):101–133, January 2018.

[BNN+10] Paulo S. L. M. Barreto, Ventzislav Nikov, Svetla Nikova, Vincent Rijmen, and Elmar Tischhauser. Whirlwind: A new cryptographic hash function. *Designs, Codes and Cryptography*, 56(2–3):141–162, 2010.

[BR22] Navid Ghaedi Bardeh and Vincent Rijmen. New key-recovery attack on reduced-round AES. *IACR Trans. Symm. Cryptol.*, 2022(2):43–62, 2022.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, January 1991.

[DFJ13] Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved key recovery attacks on reduced-round AES in the single-key setting. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 371–387. Springer, Heidelberg, May 2013.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved single-key attacks on 8-round AES-192 and AES-256. In Masayuki Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 158–176. Springer, Heidelberg, December 2010.

[DR09] Joan Daemen and Vincent Rijmen. New criteria for linear maps in aes-like ciphers. *Cryptogr. Commun.*, 1(1):47–69, 2009.

[DS08] Hüseyin Demirci and Ali Aydin Selçuk. A meet-in-the-middle attack on 8-round AES. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 116–126. Springer, Heidelberg, February 2008.

[G+21] Lorenzo Grassi et al. Poseidon: A new hash function for zero-knowledge proof systems. In *30th USENIX Security Symposium*, pages 519–535. USENIX Association, 2021.

[GPR+19] Kishan Chand Gupta, Sumit Kumar Pandey, Indranil Ghosh Ray, , and Susanta Samanta. Cryptographically significant MDS matrices over finite fields: a brief survey and some generalized results. *Advances in Mathematics of Communications*, 13(4):779–843, 2019.

[GSA+19] Gülsüm Gözde Güzel, Muharrem Tolga Sakalli, Sedat Akleylek, Vincent Rijmen, and Yasemin Cengellenmis. A new matrix form to generate all 3×3 involutory MDS matrices over $\mathbb{F}_2^m$. *Inf. Process. Lett.*, 147:61–68, 2019.

[JLG25] Sonu Jha, Shun Li, and Danilo Gligoroski. Construction of hadamard-based mixcolumns matrices resistant to related-differential cryptanalysis. *IACR Commun. Cryptol.*, 2(1):37, 2025.

[KMS+24] Yogesh Kumar, P.R. Mishra, Susanta Samanta, Kishan Chand Gupta, and Atul Gaur. Construction of all MDS and involutory MDS matrices. *Advances in Mathematics of Communications*, 18(6):1547–1566, 2024.

[KYS26] Yogesh Kumar, Akshay Ankush Yadav, and Susanta Samanta. Analyzing linear layers in related-differential cryptanalysis. arXiv ePrints 2605.27535, 2026.

[LDKK08] Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New impossible differential attacks on AES. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *INDOCRYPT 2008*, volume 5365 of *LNCS*, pages 279–293. Springer, Heidelberg, December 2008.

[Leu23] Gaëtan Leurent. MDS matrices. In *Symmetric Cryptography 1: Design and Security Proofs*, pages 99–109. Wiley Online Library, 2023.

[LP21] Gaëtan Leurent and Clara Pernot. New representations of the AES key schedule. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part I*, volume 12696 of *LNCS*, pages 54–84. Springer, Heidelberg, October 2021.

[Mat94] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 386–397. Springer, Heidelberg, May 1994.

[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.

[Rot06] Ron M. Roth. Introduction to Coding Theory. Cambridge, UK: Cambridge University Press, 2006.

[SLS+23] Alan Szepieniec, Alexander Lemmens, Jan Ferdinand Sauer, Bobbin Threadbare, and Al-Kindi. The tip5 hash function for recursive STARKs. Cryptology ePrint Archive, Paper 2023/107, 2023.