A New Matrix Form to Generate All 3×3 Involutory MDS Matrices over $\mathbb{F}_{2^m}$

Gülsüm Gözde Güzel · Muharrem Tolga
Sakallı · Sedat Akleylek · Vincent
Rijmen · Yasemin Çengellenmiş

Received: date / Accepted: date

Abstract In this paper, we propose a new matrix form to generate all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$ and prove that the number of all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$ is $(2^m - 1)^2 \cdot (2^m - 2) \cdot (2^m - 4)$, where $m > 2$. Moreover, we give 3×3 involutory and MDS matrices over $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ defined by the irreducible polynomials $x^3 + x + 1$, $x^4 + x + 1$ and $x^8 + x^7 + x^6 + x + 1$, respectively, by considering the minimum XOR count, which is a metric used in the estimation of hardware implementation cost. Finally, we provide the maximum number of 1s in 3×3 involutory MDS matrices.

Keywords MDS matrices · Diffusion layer · Involutory matrices

Mathematics Subject Classification (2000) 94A60

G.G. Güzel
Computational Sciences, Trakya University, Edirne, Turkey
E-mail: ggozdeguzel@trakya.edu.tr

T. Sakallı
Department of Computer Engineering, Trakya University, Edirne, Turkey
E-mail: tolga@trakya.edu.tr

S. Akleylek
Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey
E-mail: sedat.akleylek@bil.omu.edu.tr

V. Rijmen
Department of ESAT/COSIC, KU Leuven and imec, Belgium
E-mail: vincent.rijmen@esat.kuleuven.be

Y. Çengellenmiş
Department of Mathematics, Trakya University, Edirne, Turkey
E-mail: ycengel@trakya.edu.tr

1 Introduction

Maximum Distance Separable (MDS) matrices derived from MDS codes are used as the main part of diffusion layers in the design of cryptographic primitives like block ciphers and hash functions because they provide maximum diffusion, which is one of the two important cryptographic properties (the other is confusion) introduced by Claude Shannon [0]. MDS matrices improve the avalanche characteristics of cryptographic primitives and help to provide security against differential [0] and linear cryptanalysis [0] along with the use of a confusion layer (or non-linear layer). On the other hand, involutory diffusion layers (MDS matrices) have advantages in the design of block ciphers since they have a major contribution to a block cipher to be implemented by the same module and the same implementation cost in encryption and decryption processes. Therefore, the construction of involutory diffusion layers (MDS matrices) with low cost implementation properties is an interesting and a good research direction in the design of (lightweight) block ciphers.

In the literature, there are several construction methods of MDS matrices that are based on some special matrix types such as circulant matrices, Hadamard matrices, Cauchy matrices [0], Vandermonde matrices [0,0], companion matrices [0,0] and Toeplitz matrices [0,0]. Recently, circulant involutory MDS matrices over $GL(4, \mathbb{F}_2)$ and $GL(8, \mathbb{F}_2)$ have been proposed in [0] and generalization of circulant matrices (a new form called cyclic matrices) have been given in [0]. The studies for construction of involutory MDS matrices over $\mathbb{F}_{2^m}$ are mainly based on Hadamard matrices allowing to construct involutory matrices easily and the exhaustive search algorithm given in [0]. In [0], subfield-Hadamard construction was given, which is based on dividing each element in two parts, i.e., (involutory) MDS matrices over $\mathbb{F}_{2^k}$ are used to obtain (involutory) MDS matrices over $\mathbb{F}_{2^{2k}}$. In [0], a new matrix type called Generalized Hadamard (GHadamard) matrix, which generates new types of $k \times k$ (where $k = 2^t$) (involutory) MDS matrices efficiently, was proposed. The idea can also be applied to $k \times k$ (involutory) MDS matrices, where k is not a necessarily power of 2. The methods for the construction of MDS matrices given in the literature are mainly based on search except for the methods based on Cauchy matrices and Vandermonde matrices. On the other hand, GHadamard matrix type provides a hybrid construction, which requires (involutory) MDS matrices to generate new types of (involutory) MDS matrices.

In this paper, we present a new matrix form for 3×3 matrices, which can be used to generate all involutory and MDS matrices over $\mathbb{F}_{2^m}$. Then, we generate 3×3 matrices over $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ to obtain lightweight matrices in terms of the metric XOR count, which is introduced in [0] and used to estimate hardware implementation cost of a diffusion matrix.

1.1 Motivation and Contribution

There are several studies on $2^t \times 2^t$ MDS matrices with efficient implementation properties. Other dimensions have not been deeply studied. In [0], the lightest 3×3 involutory MDS matrices over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ in left-circulant form were given. Determining the requirements of being 3×3 involutory MDS is an interesting problem since one can use these properties to construct large MDS matrices efficiently. 3×3 (involutory) MDS matrices can be used in the design of (lightweight) block ciphers and hash functions with unusual block and key sizes. For example, in [0], an iterated block cipher for constrained platforms named Curupira was proposed. Curupira uses 96-bit plaintext blocks with the keys of 96, 144 or 192 bits. Plaintext, subkeys and also ciphertext are formed in a $3 \times N$ matrix of bytes, where N is the number of 24-bit words. The diffusion layer of Curupira is a 3×3 MDS matrix over $\mathbb{F}_{2^8}$. The contributions of this paper can be classified as follows:

- We define a new way to construct 3×3 involutory MDS matrices over any binary field extension.
- We count the number of 3×3 involutory MDS matrices over $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$.
- We provide the maximum number of 1s in 3×3 involutory MDS matrices and improve the upper bound given in [0] from 6 to 3.
- We improve the results of [0], i.e., we provide 3×3 involutory MDS matrices over $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ with the lowest known XOR counts.

1.2 Organization

This paper is organized as follows: In Section , we give some basic definitions related to the paper and MDS matrices. In Section , we propose a new 3×3 matrix form to be used in generating all involutory and MDS matrices in this size and provide some examples by considering XOR count. Then, we present experimental results for 3×3 involutory and MDS matrices with the lowest known XOR counts and compare them with the previous results in Section . We conclude in Section .

2 Preliminaries

In this paper, we focus on generating all 3×3 involutory and MDS matrices over the finite field $\mathbb{F}_{2^m}$, where the finite field $\mathbb{F}_{2^m}$ has 2^m elements and is defined by an irreducible polynomial $p(x)$ of degree m . Hence, we can denote the finite field $\mathbb{F}_{2^m}$ by $\mathbb{F}_2[x]/(p(x))$ and represent any element of $\mathbb{F}_{2^m}$ by $c_{m-1}\alpha^{m-1} + c_{m-2}\alpha^{m-2} + \dots + c_1\alpha + c_0$ with $c_i \in \mathbb{F}_2$, where α is a root of $p(x)$ (and also primitive element of $\mathbb{F}_{2^m}$). In this paper, for simplicity, we denote the finite field $\mathbb{F}_{2^m}$ defined by irreducible polynomial $p(x)$ as $\mathbb{F}_{2^m}/p(x)$. We also use hexadecimal notation or powers of a primitive element when representing the

elements of $\mathbb{F}_{2^m}$ and the irreducible polynomial $p(x)$ in hexadecimal notation when denoting $\mathbb{F}_{2^m}/p(x)$. For example, 1011, a 4-bit string, corresponds to the polynomial $\alpha^3 + \alpha + 1$ in $\mathbb{F}_{2^4}$ and it can be represented by 0xb in hexadecimal notation. In addition, when denoting $\mathbb{F}_{2^4}/0x13$, 0x13 stands for the irreducible polynomial $p(x) = x^4 + x + 1$.

An $[n, k, d]$ code C is MDS if it meets the Singleton bound $d = n - k + 1$, where n is the length of the code C , k is the number of rows of generating matrix of C and d is the minimum distance of the code C . MDS matrices are derived from MDS codes. They have the maximum differential and linear branch number ($k + 1$ for $k \times k$ MDS matrices) [0], which help to design block ciphers resistant against differential and linear cryptanalysis. Some important properties of MDS matrices, recalled in [0], are as follows:

1. A $k \times k$ matrix M is MDS if and only if every square sub-matrix of M is non-singular.
2. The MDS property of a $k \times k$ matrix M is preserved under the transpose operation.
3. The MDS property of a $k \times k$ matrix M is preserved upon multiplication of a row/column of M by a non-zero constant $c \in \mathbb{F}_{2^m}$.

The number of XOR operations required in hardware implementations or lightweightness of a given matrix is measured by using XOR count which can be grouped into two groups: d-XOR and s-XOR. The main difference between d-XOR and s-XOR count is based on the usage of temporary registers. As a result, $s\text{-XOR}(a) \leq d\text{-XOR}(a)$. In Definition , the naive one (also called d-XOR [0]) introduced in [0] is given.

Definition 1 $\text{XOR}(a)$ (d-XOR (a)) is the number of XORs required to implement the multiplication of a finite field element $a \in \mathbb{F}_{2^m}/p(x)$ and defined by the Hamming weight of corresponding $m \times m$ multiplication binary matrix (companion matrix of $p(x)$) minus m .

In order to improve this single multiplication approach, reusing intermediate results namely s-XOR was proposed in [0,0]. In Definition , s-XOR is given.

Definition 2 $s\text{-XOR}(a)$ is the minimum number of XORs needed to implement the $m \times m$ multiplication binary matrix after over all implementation and performing a sequence of XOR instructions.

There are two main optimization techniques to improve the number of the required XOR gates: local and global optimization. In local optimization, every element of the $k \times k$ matrix over $\mathbb{F}_{2^m}$ is considered, whereas, in global optimization the whole matrix is used as a binary matrix. Then, the problem returns to the optimization of $mk \times mk$ binary matrix. The idea of global optimization is the problem of finding shortest linear straight-line program over a binary field [0,0]. Global optimization is divided into two main approaches: cancellation-free programs and heuristic. In cancellation-free programs, common subexpressions are iteratively eliminated [0] and this helps to reduce the

required number of XORs. In [0,0], the authors focused on the optimization of linear operations over the binary field with cancellations. Moreover, there are several studies on finding good linear straight line programs to construct better MDS matrices in view of global optimization [0,0,0]. In this paper, we present the implementation details by focusing on XOR count (or d-XOR) and the cancellation-free approach given in [0].

In [0], the authors try to find MDS matrices with low XOR counts for any given basis. In [0], the authors study the behavior of the XOR count distributions for different bases of finite field and state that the choice of basis under the same irreducible polynomial affects the XOR count distribution. In this paper, we propose a new matrix form for generating all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$. In this context, we generate and find 3×3 involutory and MDS matrices over $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ with lowest known XOR counts by considering polynomial basis. This is because of the fact that it is widely used in the implementation and the finite field elements tend to have low XOR counts. Therefore, we choose the irreducible polynomials with the highest deviations regarding the XOR count distribution by following the recommendation of the paper [0] since the choice of irreducible polynomial generating the finite field also affects the XOR count distribution. Hence, the irreducible polynomials chosen are respectively **0xb** ($p(x) = x^3 + x + 1$), **0x13** ($p(x) = x^4 + x + 1$) and **0x1c3** ($p(x) = x^8 + x^7 + x^6 + x + 1$) for the finite fields $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$. Some examples are also provided by using the irreducible polynomials **0x1f** ($p(x) = x^4 + x^3 + x^2 + x + 1$) and **0x165** ($p(x) = x^8 + x^6 + x^5 + x^2 + 1$) for the finite fields $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$, respectively.

In Table , we give XOR counts for $\mathbb{F}_{2^3}$. The XOR counts of the elements in Table are computed by modular multiplication of two polynomials over the selected finite field. Let $a = a_2\alpha^2 + a_1\alpha + a_0$ and $b = b_2\alpha^2 + b_1\alpha + b_0$ be two polynomials over $\mathbb{F}_{2^3}/\mathbf{0xb}$. Then, the coefficients vector of a and b are $a = (a_2, a_1, a_0)$ and $b = (b_2, b_1, b_0)$, respectively. For example, assume that $a = \alpha$. Then, $a \cdot b = (0, 1, 0) \cdot (b_2, b_1, b_0) = (b_1, b_0 \oplus b_2, b_2)$ in which there is 1 XOR and therefore the XOR count for multiplication by α ($\text{XOR}(\alpha)$) is 1. Also, the multiplication binary matrix of the element α with an arbitrary element b (in the form of coefficients vector) can be written as follows:

Table 1 XOR counts for $\mathbb{F}_{2^3}$ [0]

	Field Element	0xb	0xd
0	0	0	0
0x1	1	0	0
0x2	α	1	1
0x3	$\alpha + 1$	4	2
0x4	α^2	2	3
0x5	$\alpha^2 + 1$	1	4
0x6	$\alpha^2 + \alpha$	4	1
0x7	$\alpha^2 + \alpha + 1$	3	4

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} b_2 \\ b_0 \oplus b_2 \\ b_1 \end{bmatrix}.$$

Consider a 3×3 left circulant involutory MDS matrix $M = \begin{bmatrix} 0\mathbf{x}3 & 0\mathbf{x}7 & 0\mathbf{x}5 \\ 0\mathbf{x}7 & 0\mathbf{x}5 & 0\mathbf{x}3 \\ 0\mathbf{x}5 & 0\mathbf{x}3 & 0\mathbf{x}7 \end{bmatrix}$

over $\mathbb{F}_{2^3}/0\mathbf{x}\mathbf{b}$. The XOR count of M is obtained as follows: According to Table , multiplication by $0\mathbf{x}3$, $0\mathbf{x}7$ and $0\mathbf{x}5$ needs 4, 3 and 1 XOR operations, respectively. The XOR sum of all multiplication results also requires $2 \cdot 3 = 6$ XOR operations for each row. Then, the XOR count for each row is obtained as $(4 + 3 + 1) + 2 \cdot 3 = 14$. As a result, the XOR count of M over $\mathbb{F}_{2^3}/0\mathbf{x}\mathbf{b}$ is $14 \cdot 3 = 42$.

3 A New 3×3 Matrix Form

In this section, we define a new matrix form for generating all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$. We also show that the number of all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$ is $(2^m - 1)^2 \cdot (2^m - 2) \cdot (2^m - 4)$. Using the proposed matrix form, we present two examples of 3×3 involutory and MDS matrices over $\mathbb{F}_{2^8}$, which are also given in the literature. In Theorem , we give a new matrix form to be used in generating 3×3 involutory matrices over $\mathbb{F}_{2^m}$.

Theorem 1 Let $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ be a 3×3 matrix over $\mathbb{F}_{2^m}$. If the matrix

A is involutory, then the elements of A can be expressed by using only two diagonal elements a_{11} and a_{22} as follows: $a_{12} = (a_{11} + 1)b_0$, $a_{13} = (a_{11} + 1)b_1$, $a_{21} = (a_{22} + 1)b_0^{-1}$, $a_{23} = (a_{22} + 1)b_0^{-1}b_1$, $a_{31} = (a_{11} + a_{22})b_1^{-1}$, $a_{32} = (a_{11} + a_{22})b_1^{-1}b_0$ and $a_{33} = a_{11} + a_{22} + 1$, where $a_{11} \neq a_{22}$ and $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$. Hence, the proposed 3×3 involutory matrix form $(IM)_{3 \times 3}$ is in the following form:

$$(IM)_{3 \times 3} = \begin{bmatrix} a_{11} & (a_{11} + 1)b_0 & (a_{11} + 1)b_1 \\ (a_{22} + 1)b_0^{-1} & a_{22} & (a_{22} + 1)b_0^{-1}b_1 \\ (a_{11} + a_{22})b_1^{-1} & (a_{11} + a_{22})b_1^{-1}b_0 & a_{11} + a_{22} + 1 \end{bmatrix}.$$

Proof Let the matrix $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ be involutory and let $c_{ij} = \sum_{k=1}^3 a_{ik}a_{kj}$

denote the elements of A^2 for $i, j = 1, 2, 3$. Then $A^2 = I$, where I is the 3×3 identity matrix. If $i = j$, then $c_{ij} = 1$. Otherwise, $c_{ij} = 0$. Hence, we get the following equations:

$$a_{11}^2 + a_{12}a_{21} + a_{13}a_{31} = 1 \quad (1)$$

$$a_{21}a_{12} + a_{22}^2 + a_{23}a_{32} = 1 \quad (2)$$

$$a_{31}a_{13} + a_{32}a_{23} + a_{33}^2 = 1 \quad (3)$$

$$a_{11}a_{12} + a_{12}a_{22} + a_{13}a_{32} = 0 \quad (4)$$

$$a_{11}a_{13} + a_{12}a_{23} + a_{13}a_{33} = 0 \quad (5)$$

$$a_{21}a_{11} + a_{22}a_{21} + a_{23}a_{31} = 0 \quad (6)$$

$$a_{21}a_{13} + a_{22}a_{23} + a_{23}a_{33} = 0 \quad (7)$$

$$a_{31}a_{11} + a_{32}a_{21} + a_{33}a_{31} = 0 \quad (8)$$

$$a_{31}a_{12} + a_{32}a_{22} + a_{33}a_{32} = 0 \quad (9)$$

By adding the equations (1), (2) and (3) side by side, we have $a_{11}^2 + a_{22}^2 + a_{33}^2 = 1$. In $\mathbb{F}_{2^m}$, we get

$$a_{11} + a_{22} + a_{33} = 1 \quad (10)$$

From the equations (4), (5), (6), (7), (8) and (9) we have:

$$a_{12}(a_{11} + a_{22}) = a_{13}a_{32} \quad (11)$$

$$a_{13}(a_{11} + a_{33}) = a_{12}a_{23} \quad (12)$$

$$a_{21}(a_{11} + a_{22}) = a_{23}a_{31} \quad (13)$$

$$a_{23}(a_{22} + a_{33}) = a_{21}a_{13} \quad (14)$$

$$a_{31}(a_{11} + a_{33}) = a_{32}a_{21} \quad (15)$$

$$a_{32}(a_{22} + a_{33}) = a_{31}a_{12} \quad (16)$$

After multiplying the equations (11) and (13), the equations (12) and (15), and the equations (14) and (16) side by side, we have the following equations, respectively :

$$a_{12}a_{21}(a_{11} + a_{22})^2 = a_{13}a_{31}a_{32}a_{23} \quad (17)$$

$$a_{13}a_{31}(a_{11} + a_{33})^2 = a_{12}a_{21}a_{32}a_{23} \quad (18)$$

$$a_{23}a_{32}(a_{22} + a_{33})^2 = a_{21}a_{12}a_{13}a_{31} \quad (19)$$

After multiplying the equations (18) and (19), we have $(a_{11} + a_{33})^2(a_{22} + a_{33})^2 = (a_{12}a_{21})^2$ and obtain $a_{12}a_{21} = (a_{11} + a_{33})(a_{22} + a_{33})$. By using the equation (10), we obtain a_{12} and a_{21} as follows: $a_{12} = (a_{11} + 1)b_0$, $a_{21} = (a_{22} + 1)b_0^{-1}$, where $b_0 \in \mathbb{F}_{2^m} - \{0\}$. Using the given restriction $a_{11} \neq a_{22}$, we can easily get that the sum of a_{11} and a_{22} cannot be equal to 0. Therefore, the right sides of the equations (11) and (13) are not equal to 0 since we are working in binary field extension. By considering these truths, the elements a_{13} , a_{31} , a_{32} and a_{23} can be derived from the equations, which are obtained after the following multiplications of the equations (17) and (19), and the equations

(17) and (18). Hence, we obtain $a_{13} = (a_{11} + 1)b_1$ and $a_{31} = (a_{22} + 1)b_1^{-1}$, where $b_1 \in \mathbb{F}_{2^m} - \{0\}$, by multiplying the equations (17) and (19), and using the equation (10). Similarly, after multiplying the equations (17) and (18), we obtain $a_{23} = (a_{22} + 1)b_0^{-1}b_1$ by using the equations (10) and (14) and $a_{32} = (a_{11} + a_{22})b_1^{-1}b_0$ by using the equations (10) and (16), respectively, where $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$. Finally, we obtain the desired form.

Remark 1 The proposed matrix form $(IM)_{3 \times 3}$ given in Theorem generates all 3×3 involutory matrices except for involutory matrices generated by $(IM)_{3 \times 3}$ with the restriction $a_{11} = a_{22}$. Also, such involutory matrices generated with this restriction cannot be MDS. In Proposition , we give $(IM)_{3 \times 3}$ with the additional restrictions for generating all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$.

Proposition 1 *Let $(IM)_{3 \times 3}$ be as in Theorem . Then, any 3×3 involutory matrix over $\mathbb{F}_{2^m}$ generated by $(IM)_{3 \times 3}$ satisfying the restrictions $a_{11} \neq a_{22}$, $a_{11}, a_{22} \neq 0$, $a_{11}, a_{22} \neq 1$, $a_{11} + a_{22} \neq 1$ (and for any $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$) is MDS. Thus, the number of all 3×3 involutory MDS matrices over $\mathbb{F}_{2^m}$ is $(2^m - 1)^2 \cdot (2^m - 2) \cdot (2^m - 4)$, where $m > 2$.*

Proof Recall that a $k \times k$ matrix M is MDS if and only if every square sub-matrix of M is non-singular. In this context, involutory matrices generated by $(IM)_{3 \times 3}$ given in Theorem are MDS by considering the restrictions, which are $a_{11} \neq a_{22}$, $a_{11} \neq 0$, $a_{22} \neq 0$, $a_{11} \neq 1$, $a_{22} \neq 1$, $a_{11} + a_{22} \neq 1$ and for any $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$. This is because of the fact that the elements of the matrix form $(IM)_{3 \times 3}$ are not equal to zero, which corresponds to the determinants of 1×1 square sub-matrices of $(IM)_{3 \times 3}$, and also the determinants of 2×2 square sub-matrices of $(IM)_{3 \times 3}$ are not equal to zero. These 2×2 square sub-matrices of $(IM)_{3 \times 3}$ and their determinants are given as follows:

$$\begin{vmatrix} a_{11} & (a_{11} + 1)b_0 \\ (a_{22} + 1)b_0^{-1} & a_{22} \end{vmatrix} = a_{11} + a_{22} + 1 \neq 0$$

$$\begin{vmatrix} a_{11} & (a_{11} + 1)b_1 \\ (a_{22} + 1)b_0^{-1} & (a_{22} + 1)b_0^{-1}b_1 \end{vmatrix} = b_0^{-1}b_1(a_{22} + 1) \neq 0$$

$$\begin{vmatrix} (a_{11} + 1)b_0 & (a_{11} + 1)b_1 \\ a_{22} & (a_{22} + 1)b_0^{-1}b_1 \end{vmatrix} = b_1(a_{11} + 1) \neq 0$$

$$\begin{vmatrix} a_{11} & (a_{11} + 1)b_0 \\ (a_{11} + a_{22})b_1^{-1} & (a_{11} + a_{22})b_1^{-1}b_0 \end{vmatrix} = b_1^{-1}b_0(a_{11} + a_{22}) \neq 0$$

$$\begin{vmatrix} a_{11} & (a_{11} + 1)b_1 \\ (a_{11} + a_{22})b_1^{-1} & a_{11} + a_{22} + 1 \end{vmatrix} = a_{22} \neq 0$$

$$\begin{vmatrix} (a_{11} + 1)b_0 & (a_{11} + 1)b_1 \\ (a_{11} + a_{22})b_1^{-1}b_0 & a_{11} + a_{22} + 1 \end{vmatrix} = b_0(a_{11} + 1) \neq 0$$

$$\begin{vmatrix} (a_{22} + 1)b_0^{-1} & a_{22} \\ (a_{11} + a_{22})b_1^{-1} & (a_{11} + a_{22})b_1^{-1}b_0 \end{vmatrix} = b_1^{-1}(a_{11} + a_{22}) \neq 0$$

$$\begin{vmatrix} (a_{22} + 1)b_0^{-1} & (a_{22} + 1)b_0^{-1}b_1 \\ (a_{11} + a_{22})b_1^{-1} & a_{11} + a_{22} + 1 \end{vmatrix} = b_0^{-1}(a_{22} + 1) \neq 0$$

$$\begin{vmatrix} a_{22} & (a_{22} + 1)b_0^{-1}b_1 \\ (a_{11} + a_{22})b_1^{-1}b_0 & a_{11} + a_{22} + 1 \end{vmatrix} = a_{11} \neq 0$$

The matrix form $(IM)_{3 \times 3}$ with the given restrictions is expressed by only the diagonal elements a_{11} , a_{22} and any $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$ (Note that if b_0 and b_1 are any non-zero elements, the MDS property of involutory matrices is preserved because these elements are multiplier in the final determinant expressions of sub-matrices and do not affect determinant values in terms of being equal to non-zero). Therefore, the number of choices for b_0, b_1 is $(2^m - 1)^2$. By the given restrictions, the element a_{11} cannot be equal to zero and 1. Then, the number of choices for the element a_{11} is $2^m - 2$. The element a_{22} should be different from the elements a_{11} and $a_{11} + 1$ in order to choose distinct diagonal elements and at the same time their sum equal to 1, which means that the number of choices for the element a_{22} is $2^m - 4$ for $m > 2$. Thus, the number of all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$ is $(2^m - 1)^2 \cdot (2^m - 2) \cdot (2^m - 4)$, where $m > 2$.

By using Theorem and Proposition , we give the proposed matrix form $(IM)_{3 \times 3}$ in Definition in order to represent 3×3 involutory and MDS matrices easily.

Definition 3 The matrix form $IM_{3 \times 3}(a_{11}, a_{22}, b_0, b_1)$ for generating all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$ can be defined as follows:

$$(IM)_{3 \times 3} = \begin{bmatrix} a_{11} & (a_{11} + 1)b_0 & (a_{11} + 1)b_1 \\ (a_{22} + 1)b_0^{-1} & a_{22} & (a_{22} + 1)b_0^{-1}b_1 \\ (a_{11} + a_{22})b_1^{-1} & (a_{11} + a_{22})b_1^{-1}b_0 & a_{11} + a_{22} + 1 \end{bmatrix}$$

where $a_{11} \neq a_{22}$, $a_{11}, a_{22} \neq 0$, $a_{11}, a_{22} \neq 1$, $a_{11} + a_{22} \neq 1$ and $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$.

In Example , we generate a 3×3 involutory MDS matrix over $\mathbb{F}_{2^8}$ by using the proposed matrix form, which is also constructed from a Vandermonde matrix in [0].

Example 1 Let $\mathbb{F}_{2^8}$ be generated by the root α which is a root of the primitive polynomial $0x11d$. Consider $IM_{3 \times 3}(\alpha, \alpha^{26}, \alpha^{173}, \alpha^{232})$ over $\mathbb{F}_{2^8}/0x11d$. Then, it can be expressed as follows:

$$IM_{3 \times 3}(\alpha, \alpha^{26}, \alpha^{173}, \alpha^{232}) = \begin{bmatrix} \alpha & \alpha^{198} & \alpha^2 \\ \alpha^{25} & \alpha^{26} & \alpha^2 \\ \alpha^{25} & \alpha^{198} & \alpha^{50} \end{bmatrix} = \begin{bmatrix} 0x02 & 0x07 & 0x04 \\ 0x03 & 0x06 & 0x04 \\ 0x03 & 0x07 & 0x05 \end{bmatrix}$$

which is 3×3 involutory and MDS matrix over $\mathbb{F}_{2^8}/0x11d$.

In Example , we generate a 3×3 involutory MDS matrix over $\mathbb{F}_{2^8}$ by using the proposed matrix form, which is also obtained by a left circulant matrix in [0].

Example 2 Let $\mathbb{F}_{2^8}$ be generated by the root α which is a root of the primitive polynomial $0x169$. Consider $IM_{3 \times 3}(\alpha^{253}, \alpha^{250}, \alpha^3, \alpha^{220})$ over $\mathbb{F}_{2^8}/0x169$. Then, it can be expressed as follows:

$$IM_{3 \times 3}(\alpha^{253}, \alpha^{250}, \alpha^3, \alpha^{220}) = \begin{bmatrix} \alpha^{253} & \alpha^{33} & \alpha^{250} \\ \alpha^{33} & \alpha^{250} & \alpha^{253} \\ \alpha^{250} & \alpha^{253} & \alpha^{33} \end{bmatrix} = \begin{bmatrix} 0x5a & 0x0a & 0x51 \\ 0x0a & 0x51 & 0x5a \\ 0x51 & 0x5a & 0x0a \end{bmatrix}$$

which is 3×3 involutory and MDS matrix over $\mathbb{F}_{2^8}/0x169$ with XOR count 138 ($= 90 + 3 \cdot 2 \cdot 8$) since the XOR counts of α^{253} , α^{33} and α^{250} are 6, 11 and 13, respectively.

4 Experimental Results for 3×3 Involutory and MDS Matrices with the Lowest Known XOR counts

In this section, we obtain 3×3 involutory and MDS matrices over $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}/0x1c3$ with the lowest known XOR counts. By Proposition , there are 1176, 37800 and $\approx 2^{31.95}$ 3×3 involutory and MDS matrices over $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$, respectively. We generated all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^3}/0xb$, $\mathbb{F}_{2^4}/0x13$ and $\mathbb{F}_{2^8}/0x1c3$ and checked the ones with the minimum XOR count. We respectively identified 24, 12 and 24 3×3 involutory and MDS matrices over $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ with the lowest known XOR counts. In Example , we present one of these 3×3 involutory MDS matrices over $\mathbb{F}_{2^3}/0xb$ generated by using the proposed matrix form. The other 3×3 involutory MDS matrices over $\mathbb{F}_{2^3}/0xb$ with the same XOR count are listed in Appendix.

Remark 2 Because of the fact that we generated all 3×3 involutory MDS matrices for the finite field $\mathbb{F}_{2^8}$ defined by the primitive polynomial $0x1c3$, there might be better matrices in view of XOR count for the finite field $\mathbb{F}_{2^8}$ defined by other irreducible polynomials. For the finite fields $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^4}$, we present 3×3 involutory MDS matrices with the lowest known XOR counts by considering the primitive polynomials $x^3 + x + 1$ and $x^4 + x + 1$ because the

primitive polynomials x^3+x^2+1 and x^4+x^3+1 are, respectively, the reciprocal counterpart of the primitive polynomials x^3+x+1 and x^4+x+1 , and the elements of the reciprocal polynomials have the same XOR count distribution as given in Theorem 2 of [0]. Also, we generated all 3×3 involutory MDS matrices over $\mathbb{F}_{2^4}$ defined by the irreducible polynomial $x^4+x^3+x^2+x+1$ but the experimental results were not satisfactory for this pentanomial. Hence, in this study, we present 3×3 involutory MDS matrices over the finite fields $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^4}$ with the lowest known XOR counts. On the other hand, better 3×3 involutory and MDS matrices in view of XOR count may be obtained by applying some global optimization techniques to these matrices or by looking at other bases.

Example 3 Let $\mathbb{F}_{2^3}$ be generated by the root α which is a root of the primitive polynomial $0xb$. Consider $IM_{3 \times 3}(\alpha, \alpha^2, \alpha^4, \alpha^4)$ over $\mathbb{F}_{2^3}/0xb$. Then, it can be expressed as follows:

$$IM_{3 \times 3}(\alpha, \alpha^2, \alpha^4, \alpha^4) = \begin{bmatrix} \alpha & 1 & 1 \\ \alpha^2 & \alpha^2 & \alpha^6 \\ 1 & \alpha^4 & \alpha^5 \end{bmatrix} = \begin{bmatrix} 0x2 & 0x1 & 0x1 \\ 0x4 & 0x4 & 0x5 \\ 0x1 & 0x6 & 0x7 \end{bmatrix}$$

which is 3×3 involutory and MDS matrix over $\mathbb{F}_{2^3}/0xb$ with XOR count 31 ($= 13 + 3 \cdot 2 \cdot 3$) since the XOR counts of $1, \alpha, \alpha^2, \alpha^4, \alpha^5$ and α^6 are 0, 1, 2, 4, 3 and 1, respectively. When one uses the idea of eliminating common subexpressions given in [0], one needs 19 XORs.

In Example , we present one of the 3×3 involutory MDS matrices over $\mathbb{F}_{2^4}$ with the lowest known XOR count, which is generated by using the proposed matrix form. The other 3×3 involutory MDS matrices over $\mathbb{F}_{2^4}/0x13$ with the same XOR count are listed in Appendix.

Example 4 Let $\mathbb{F}_{2^4}$ be generated by the root α which is a root of the primitive polynomial $0x13$. Consider $IM_{3 \times 3}(\alpha^3, \alpha^6, 1, \alpha^2)$ over $\mathbb{F}_{2^4}/0x13$. Then, it can be expressed as follows:

$$IM_{3 \times 3}(\alpha^3, \alpha^6, 1, \alpha^2) = \begin{bmatrix} \alpha^3 & \alpha^{14} & \alpha \\ \alpha^{13} & \alpha^6 & 1 \\ 1 & 1 & \alpha^8 \end{bmatrix} = \begin{bmatrix} 0x8 & 0x9 & 0x2 \\ 0xd & 0xc & 0x1 \\ 0x1 & 0x1 & 0x5 \end{bmatrix}$$

which is 3×3 involutory and MDS matrix over $\mathbb{F}_{2^4}/0x13$ with XOR count 43 ($= 19 + 3 \cdot 2 \cdot 4$) since the XOR counts of $1, \alpha, \alpha^3, \alpha^6, \alpha^8, \alpha^{13}$ and α^{14} are 0, 1, 3, 5, 6, 3 and 1, respectively. When one uses the idea of eliminating common subexpressions given in [0], one needs 24 XORs.

In Example , we present one of the 3×3 involutory MDS matrices over $\mathbb{F}_{2^4}/0x1f$.

Example 5 Let $\mathbb{F}_{2^4}$ be generated by the root α which is a root of the irreducible polynomial $0x1f$. Consider $IM_{3 \times 3}(\alpha + 1, (\alpha + 1)^4, (\alpha + 1)^3, 1)$ over $\mathbb{F}_{2^4}/0x1f$. Then, it can be expressed as follows:

$$IM_{3 \times 3}(\alpha + 1, (\alpha + 1)^4, (\alpha + 1)^3, 1) = \begin{bmatrix} 0x3 & 0x1 & 0x2 \\ 0x1 & 0xe & 0x1 \\ 0xd & 0x9 & 0xc \end{bmatrix}$$

which is 3×3 involutory and MDS matrix over $\mathbb{F}_{2^4}/0x1f$ with XOR count 54. When one uses the idea of eliminating common subexpressions given in [0], one needs 27 XORs.

In Example , we present one of the 3×3 involutory MDS matrices over $\mathbb{F}_{2^8}/0x1c3$ with the lowest known XOR count, which is generated by using the proposed matrix form. The other 3×3 involutory MDS matrices over $\mathbb{F}_{2^8}/0x1c3$ with the same XOR count are listed in Appendix.

Example 6 Let $\mathbb{F}_{2^8}$ be generated by the root α which is a root of the primitive polynomial $0x1c3$. Consider $IM_{3 \times 3}(\alpha^{150}, \alpha^{156}, 1, \alpha)$ over $\mathbb{F}_{2^8}/0x1c3$. Then, it can be expressed as follows:

$$IM_{3 \times 3}(\alpha^{150}, \alpha^{156}, 1, \alpha) = \begin{bmatrix} \alpha^{150} & \alpha^{58} & \alpha^{59} \\ \alpha^{254} & \alpha^{156} & 1 \\ 1 & 1 & \alpha^{157} \end{bmatrix} = \begin{bmatrix} 0xe2 & 0xe3 & 0x05 \\ 0xe1 & 0xe0 & 0x01 \\ 0x01 & 0x01 & 0x03 \end{bmatrix}$$

which is 3×3 involutory and MDS matrix over $\mathbb{F}_{2^8}/0x1c3$ with XOR count 108 ($= 60 + 3 \cdot 2 \cdot 8$) since the XOR counts of $1, \alpha^{58}, \alpha^{59}, \alpha^{150}, \alpha^{156}, \alpha^{157}$ and α^{254} are 0, 12, 11, 16, 9, 9 and 3 respectively. When one uses the idea of eliminating common subexpressions given in [0], one needs 52 XORs.

In Example , we present one of the 3×3 involutory MDS matrices over $\mathbb{F}_{2^8}/0x165$ generated by using the proposed matrix form.

Example 7 Let $\mathbb{F}_{2^8}$ be generated by the root α which is a root of the primitive polynomial $0x165$. Consider $IM_{3 \times 3}(\alpha^{173}, \alpha^{232}, 1, \alpha)$ over $\mathbb{F}_{2^8}/0x165$. Then, it can be expressed as follows:

$$IM_{3 \times 3}(\alpha^{150}, \alpha^{156}, 1, \alpha) = \begin{bmatrix} \alpha^{173} & \alpha^{210} & \alpha^{211} \\ \alpha^{254} & \alpha^{232} & 1 \\ 1 & 1 & \alpha^{233} \end{bmatrix} = \begin{bmatrix} 0xb1 & 0xb0 & 0x05 \\ 0xb2 & 0xb3 & 0x01 \\ 0x01 & 0x01 & 0x03 \end{bmatrix}$$

which is 3×3 involutory and MDS matrix over $\mathbb{F}_{2^8}/0x165$ with XOR count 111. When one uses the idea of eliminating common subexpressions given in [0], one needs 52 XORs.

In Lemma , we improve the upper bound for the number of 1s in 3×3 matrices given in [0] from 6 to 3.

Table 2 Comparison of 3×3 MDS and involutory matrices in view of XOR counts

	over $\mathbb{F}_{2^3}$		Poly	over $\mathbb{F}_{2^4}$		Poly	over $\mathbb{F}_{2^8}$		Poly
Counting	d-XOR	[0]		d-XOR	[0]		d-XOR	[0]	
Previous	-	-	-	60 [17]	40	0x1f	138 [17]	48	0x169
Ours	31 (Exam. 3)	19	0xb	43 (Exam. 4)	24	0x13	108 (Exam. 6)	52	0x1c3
Ours	-	-	-	54 (Exam. 5)	27	0x1f	111 (Exam. 7)	52	0x165

Lemma 1 *The number of 1s in 3×3 MDS and involutory matrices (given in Definition) over a binary extension field is at most 3.*

Proof By Definition , we have $a_{11} \neq a_{22}$, $a_{11}, a_{22} \neq 1$ and $a_{11} + a_{22} \neq 1$. This reduces the upper bound of the number of 1s to 6 ($=9-3$). Then, we have to consider other elements of the matrix. There are several cases to count the possible 1s in the matrix. We provide the case given in Example with the proof. The other cases can be proven in a similar manner. Let $a_{11} + a_{22} = b_1$, $a_{22} + 1 = b_1^{-1}$ and $b_0 = 1$. Then, by using $a_{11} + a_{22} + 1 \neq 0$, we have $b_1 \neq 1$. Since $a_{22} + 1 = b_1^{-1}$ and $a_{11} \neq a_{22}$, $a_{11} + 1 \neq b_1^{-1}$ for $b_1 \neq 1$ and $(a_{11} + 1)b_0 \neq 1$. Similarly, $(a_{11} + 1)b_1 = a_{11}(1 + a_{11} + a_{22}) + a_{22} \neq 1$. These results give us the maximum number of 1s in 3×3 MDS and involutory matrices, which is 3 for this case.

In Table , we compare our results with the previous studies by using d-XOR count and eliminating common subexpressions [0]. The results are checked by using the software given in [0].

5 Conclusion

In this study, we show that all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$ can be generated by using the proposed matrix form. Then, we present involutory MDS matrices over $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$ with the lowest known XOR counts and provide the maximum number of 1s in 3×3 involutory MDS matrices. In this context, the proposed matrix form can be used in the design of (lightweight) block ciphers requiring 3×3 involutory and MDS matrices in their diffusion layers with the optimal implementation properties.

If we think to express 4×4 involutory MDS matrices in a similar matrix form as in this paper, our conjecture is that there might exist a more general form (including Hadamard matrix form) or many forms (excluding Hadamard matrix form), which provide to generate 4×4 involutory matrices. But, it is difficult to express these matrices being MDS at the same time. This is because of the fact that the number of coefficients may increase to define 4×4 involutory and MDS matrices in a similar form and the number of all square sub-matrices ($\sum_{i=1}^4 \binom{4}{i}^2 = 69$), which should have non-zero determinants required for satisfying the MDS property of a 4×4 matrix, will increase. Hence, this would result in too many restrictions for 4×4 (involutory) MDS matrices and make it difficult to express these matrices in a similar matrix form as in this paper.

Acknowledgments.

Sedat Akleylek is partially supported by TÜBİTAK under grant no. EEEAG-116E279. The authors would like to express their gratitude to the anonymous reviewers for their invaluable suggestions (especially for XOR count) in putting the present study into its final form.

References

1. P. Barreto and Jr. M. Simplicio Jr, M., Curupira, a block cipher for constrained platforms, 25th Brazilian Symposium on Computer Networks and Distributed Systems (SBRC) 2007.
2. C. Beierle, T. Kranz, G. Leander, Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices, CRYPTO 2016, LNCS, vol.9814, pp. 625-653, 2016.
3. E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, CRYPTO'90, LNCS, vol. 537, pp. 2-21, 1990.
4. J. Boyar, P. Matthews, R. Peralta, Logic minimization techniques with applications to cryptology, Journal of Cryptology, vol.26(2), pp.280-312, 2013.
5. J. Boyar, R. Peralta, A new combinational logic minimization technique with applications to cryptology, SEA, LNCS, vol.6049, pp.178-189, 2010.
6. J. Daemen, V. Rijmen, The Design of Rijndael, AES - The Advanced Encryption Standard, Springer, 2002.
7. S. Duval, G. Leurent, MDS matrices with lightweight circuits, IACR Transactions on Symmetric Cryptology, vol.2018(2), pp.48-78, 2018.
8. C. Fuhs, P. Schneider-Kamp, Synthesizing shortest linear straight-line programs over $GF(2)$ using SAT, SAT, LNCS, vol.6175, pp.71-84, 2010.
9. J. Guo, T. Peyrin, A. Poschmann, The PHOTON family of lightweight hash functions, CRYPTO 2011, LNCS, vol. 6841, pp. 222-239, 2011.
10. K.C. Gupta, I.G. Ray, On constructions of MDS matrices from companion matrices for lightweight cryptography. In:CD-ARES 2013 Workshops:MoCrySEn, pp. 29-43, 2013.
11. J. Jean, T. Peyrin, S.M. Sim, J. Tourteaux, Optimizing implementations of lightweight building blocks, IACR Transactions on Symmetric Cryptology, vol.2017(4), pp.130-168, 2017.
12. P. Junod, S. Vaudenay, Perfect diffusion primitives for block ciphers, Selected Areas in Cryptography (SAC 2004), LNCS, vol.3357, pp.84-99, 2005.
13. K. Khoo, T. Peyrin, A.Y. Poschmann, and H. Yap, FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison, Cryptographic Hardware and Embedded Systems (CHES 2014), LNCS, vol. 8731, pp. 433-450, 2014.
14. T. Kranz, G. Leander, K. Stoffelen, F. Wiemer, Shorter linear straight-line programs for MDS matrices, IACR Transactions on Symmetric Cryptology, vol.2017(4), pp.188-211, 2017.
15. J. Lacan, J. Fimes, Systematic MDS erasure codes based on vandermonde matrices, IEEE Trans. Commun. Lett., vol. 8, pp. 570-572, 2004.
16. Y. Li and M. Wang, On the Construction of Lightweight Circulant Involutory MDS Matrices, Fast Software Encryption (FSE 2016), LNCS, vol.9783, pp.121-139, 2016.
17. M. Liu and S.M. Sim, Lightweight MDS Generalized Circulant Matrices, Fast Software Encryption (FSE 2016), LNCS, vol.9783, pp.101-120, 2016.
18. F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
19. M. Matsui, Linear cryptanalysis method for DES cipher, EUROCRYPT'93, LNCS, vol. 765, pp. 386-397, 1994.
20. C. Paar, Optimized arithmetic for Reed-Solomon encoders, Proceedings of IEEE International Symposium on Information Theory, pp.250, 1997.
21. M.K. Pehlivanoglu, M.T. Sakalli, S. Akleylek, N. Duru, V. Rijmen, Generalisation of Hadamard Matrix to Generate Involutory MDS Matrices for Lightweight Cryprography, IET Information Security, vol. 12(4), pp. 348-355, 2018.

-
22. M. Sajadieh, M. Dakhilalian, H. Mala, B. Omoomi, On construction of involutory MDS matrices from Vandermonde Matrices in $GF(2^q)$, Design, Codes and Cryptography, vol. 64, pp. 287-308, 2012.
 23. S. Sarkar and S.M. Sim, A deeper understanding of the XOR count distribution in the context of lightweight cryptography, AFRICACRYPT 2016, LNCS, vol.9646, pp.167-182, 2016.
 24. S. Sarkar, H. Syed, Lightweight Diffusion Layer: Importance of Toeplitz Matrices, IACR Transactions on Symmetric Cryptology, vol.2016(1), pp. 95-113, 2016.
 25. S. Sarkar, H. Syed, Analysis of Toeplitz MDS Matrices, ACISP 2017, LNCS, vol. 10343, pp. 3-18, 2017.
 26. C.E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, vol. 28, pp. 656-715, 1949.
 27. S.M. Sim, K. Khoo, F. Oggier, T. Peyrin, Lightweight MDS involution matrices, Fast Software Encryption (FSE 2015), LNCS, vol.9054, pp.471-493, 2015.
 28. A. Visconti, C.V. Schiavo, R. Peralta, Improved upper bounds for the expected circuit complexity of dense systems of linear equations over $GF(2)$, Information Processing Letters, vol.137, pp.1-5, 2018.
 29. A.M. Youssef, S. Mister, S.E. Tavares, On the Design of Linear Transformation for Substitution Permutation Encryption Networks, Proceedings of Selected Areas in Cryptography (SAC'97), pp. 40-48, 1997.

Appendix

Table 3 3×3 Involutory and MDS Matrices with the Lowest Known XOR Counts

over $\mathbb{F}_{2^3}/\text{Oxb}$				over $\mathbb{F}_{2^3}/\text{Oxb}$				over $\mathbb{F}_{2^4}/\text{Ox13}$				over $\mathbb{F}_{2^8}/\text{Ox1c3}$				over $\mathbb{F}_{2^8}/\text{Ox1c3}$			
a_{11}	a_{22}	b_0	b_1	a_{11}	a_{22}	b_0	b_1	a_{11}	a_{22}	b_0	b_1	a_{11}	a_{22}	b_0	b_1	a_{11}	a_{22}	b_0	b_1
α	α^2	α^4	α^4	α^4	α	α^2	α^2	α^3	α^6	1	α^2	α^{150}	α^{156}	1	α	α^{156}	α^{157}	α	1
α	α^2	α^6	α^4	α^4	α	α^3	α^2	α^3	α^6	α^{14}	α	α^{150}	α^{156}	α^{196}	α^{197}	α^{156}	α^{157}	α	α
α	α^4	α^4	α^6	α^4	α^6	α^2	α^2	α^3	α^8	α	α^{14}	α^{150}	α^{156}	α^{197}	α^{198}	α^{156}	α^{157}	α	α^{58}
α	α^4	α^5	1	α^4	α^6	α^2	α^3	α^3	α^8	α^2	1	α^{150}	α^{156}	α^{254}	1	α^{156}	α^{157}	α	α^{59}
α	α^5	α^4	α^4	α^5	α	α^3	1	α^6	α^3	1	α^2	α^{150}	α^{157}	1	α^{254}	α^{157}	α^{150}	1	α^{254}
α	α^5	α^4	α^6	α^5	α	α^3	α^2	α^6	α^3	α	α^2	α^{150}	α^{157}	α	1	α^{157}	α^{150}	α^{57}	α^{254}
α	α^6	1	α^5	α^5	α^2	1	α^3	α^6	α^8	α^2	1	α^{150}	α^{157}	α^{197}	α^{196}	α^{157}	α^{150}	α^{58}	α^{254}
α	α^6	α^6	α^4	α^5	α^2	α^2	α^3	α^6	α^8	α^2	α	α^{150}	α^{157}	α^{198}	α^{197}	α^{157}	α^{150}	α^{254}	α^{254}
α^2	α	α	α^5	α^6	α	1	α^5	α^8	α^3	α^{13}	α^{13}	α^{156}	α^{150}	1	α	α^{157}	α^{156}	α^{254}	1
α^2	α	α^3	1	α^6	α	α	α^5	α^8	α^3	α^{14}	α^{13}	α^{156}	α^{150}	α	α	α^{157}	α^{156}	α^{254}	α^{57}
α^2	α^5	1	α^3	α^6	α^4	α^5	1	α^8	α^6	α^{13}	α^{13}	α^{156}	α^{150}	α^{58}	α	α^{157}	α^{156}	α^{254}	α^{58}
α^2	α^5	α^5	α	α^6	α^4	α^5	α	α^8	α^6	α^{13}	α^{14}	α^{156}	α^{150}	α^{59}	α	α^{157}	α^{156}	α^{254}	α^{254}