On Lightweight 4×4 MDS Matrices over Binary Field Extensions

Fatma Büyüksaraçoğlu Sakallı[1], Özlem Aydın[1], Gökhan Tuncay[1], Meltem Kurt Pehlivanoğlu[2], Gülsüm Gözde Güzel[3], Muharrem Tolga Sakallı[1]

[1]Computer Engineering Department, Trakya University, Edirne, Turkey
[2]Computer Engineering Department, Kocaeli University, İzmit/ Kocaeli, Turkey
[3]İpsala Vocational School, Trakya University, İpsala/ Edirne, Turkey
Corresponding Author: *tolga@trakya.edu.tr*

ORCID iD: 0000-0002-6100-6655, 0000-0002-6401-4183, 0000-0002-4293-4018, 0000-0002-7581-9390, 0000-0003-0192-9797, 0000-0002-6322-0989

Research Paper Received: 16.03.2020 Revised: 12.05.2020 Accepted: 14.05.2020

Abstract—Maximum Distance Separable (MDS) matrices are used as the main part of diffusion layers in block ciphers and hash functions. MDS matrices derived from MDS codes have the maximum differential and linear branch number, which provide resistance against some well-known attacks like differential and linear cryptanalysis together with the use of a nonlinear layer (e.g. S-boxes) in a round function of a block cipher. In this paper, we introduce generic methods to generate lightweight 4×4 involutory/non-involutory MDS matrices over $\mathbb{F}_{2^m}$ and present the lightest involutory/non-involutory 4×4 MDS matrices over $\mathbb{F}_{2^4}$ (to the best of our knowledge) by considering XOR count metric, which is defined to estimate hardware implementation cost. Also, the results are obtained by using a global optimization technique, namely Boyar-Peralta algorithm.

Keywords—MDS matrices, diffusion layer, symmetric key cryptography

1. Introduction

Maximum Distance Separable (MDS) matrices are used as the main part of diffusion layers in the design of cryptographic primitives such as block ciphers and hash functions. MDS matrices are derived from MDS codes and provide maximum diffusion. Diffusion is one of the cryptographic properties (the other property is confusion) defined by Claude Shannon [1] and these two properties need to be satisfied for the overall security of symmetric key schemes. In most block ciphers, confusion and diffusion are satisfied by using Substitution boxes (shortly S-boxes) and linear transformations, respectively. In this respect, MDS matrices are used as the main part of diffusion layers (linear transformations). They have also the maximum branch number, which is an important cryptographic property and provide resistance against some well-known attacks like differential [2] and linear cryptanalysis [3] provided that they are used together with a nonlinear layer, e.g. S-boxes.

In the literature, generally, there are three construction methods to obtain MDS matrices: direct construction methods, search based methods and hybrid methods combining direct construction methods and search based methods. Direct construction methods include methods such as Cauchy matrices [4], companion matrices [5], [6] and Vandermonde matrices [7], [8]. Recently, in [9], a new direct construction method has been introduced to generate all 3×3 involutory and MDS matrices. Search based methods include using recursive structures [10], [11], hybrid structures [12] and some special matrix forms such as circulant matrices, Hadamard matrices circulant-like and Toeplitz-like matrices [13]. In [14], a new matrix form, namely Generalized Hadamard Matrix (shortly GHadamard) has been introduced. This matrix form is, in fact, a hybrid construction method and combines search based methods and direct construction methods. In addition to these studies, a new complementary method for all construction methods based on ground field structure to generate new (isomorphic) MDS matrices has recently been introduced in [15].

XOR count [16] is a metric used to evaluate the number of XOR operations required for hardware implementations or lightweightness of a given matrix. This metric can also be grouped into two groups: d-XOR (naive one) and s-XOR. The main difference between them is based on the usage of temporary registers. On the other hand, there are two different techniques to optimize MDS matrices in view of required number of XOR operations: local optimization and global optimization. In local optimization, every element of a $k \times k$ matrix over $\mathbb{F}_{2^m}$ (finite field with 2^m elements) is considered, whereas, in global optimization a $k \times k$ matrix over $\mathbb{F}_{2^m}$ is first transformed into its corresponding $mk \times mk$ binary matrix, and then this binary matrix is optimized. Shortest Linear Programs (SLP) [17] for MDS matrices are one of global optimization techniques and are heuristic techniques. In this paper, we obtain MDS matrices by using the techniques and ideas given in [9], [14] and obtain the lightest involutory/non-involutory MDS matrices (to the best of our knowledge and comparing the other MDS matrices in the literature) in view of XOR count after optimizing these matrices by SLP algorithm given in [18], namely Boyar-Peralta algorithm.

This paper is organized as follows. The notation and some background related to MDS matrices are given in Section 2. Then, in Section 3, we introduce our approach for generating new MDS matrices. Experimental results for lightweight MDS matrices are presented in Section 4 and we conclude with Section 5.

2. Preliminaries

In this paper, we focus on MDS matrices over the finite field $\mathbb{F}_{2^m}$. The finite field $\mathbb{F}_{2^m}$ has 2^m elements and is defined by an irreducible polynomial $p(x)$ of degree m over $\mathbb{F}_2$. The finite field $\mathbb{F}_{2^m}$ can be denoted by $\mathbb{F}_2[x]/p(x)$ and any element of $\mathbb{F}_{2^m}$ can be represented by $c_{m-1}\alpha^{m-1} + c_{m-2}\alpha^{m-2} + \cdots + c_1\alpha + c_0$ with $c_i \in \{0, 1\}$, where α is a primitive element of $\mathbb{F}_{2^m}$. In this paper, the finite field $\mathbb{F}_{2^m}$ defined by irreducible polynomial $p(x)$ is denoted by $\mathbb{F}_{2^m}/p(x)$ (a finite field having 2^m elements) for simplicity. Hexadecimal notation is also used when representing the elements of $\mathbb{F}_{2^m}$ and when denoting the irreducible polynomial $p(x)$ in $\mathbb{F}_{2^m}/p(x)$. For example, 1001, which is a 4-bit string and corresponds to the element $\alpha^3 + 1$ in the finite field $\mathbb{F}_{2^4}$, can be represented by `0x9` in hexadecimal notation. Similarly, `0x13` represents the irreducible polynomial $p(x) = x^4 + x + 1$ in $\mathbb{F}_{2^4}/$`0x13`.

If an $[n, k, d]$ code C 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, then the code C is MDS. MDS matrices derived from MDS codes have the maximum differential and linear branch number ($k+1$ for $k \times k$ MDS matrices) [19] and MDS matrices help design block ciphers resistant against differential and linear cryptanalysis. MDS matrices have some important properties as given below:

1 A square matrix A is MDS if and only if every square submatrix of A is nonsingular.
2 The MDS property of a matrix is preserved upon permutations of rows/columns. Similarly, multiplication of a row/column of a matrix by a nonzero constant $c \in \mathbb{F}_{2^m}$ does not affect its MDS property. In general, the minimum distance d of an $[n, k, d]$ code C with generator matrix $G = [I|A]$, where A is a $k \times (n-k)$ matrix, is preserved after applying of the above operations to A [19].
3 The MDS property of a $k \times k$ matrix M is preserved under the transpose operation

The metric XOR count is used in the estimation of the required number of XOR operations or lightweightness of a given matrix. It can be grouped into two groups: d-XOR (naive one) [16], [20] and s-XOR [21], [20].

Definition 1 ([9]): XOR (a) is the number of XORs to implement the multiplication of a finite field $a \in \mathbb{F}_{2^m}/p(x)$. It can be obtained by the Hamming weight of its corresponding $m \times m$ binary matrix minus m.

Example 1: Consider the finite field element α (or `0x2`) over $\mathbb{F}_{2^4}/$`0x13`, which is a root and a primitive element of the primitive polynomial $p(x) = x^4 + x + 1$. The 4×4 corresponding multiplication binary matrix of the finite field element α can be obtained by multiplying the element α with an arbitrary element $b \in \mathbb{F}_{2^4}/$`0x13` ($b = b_3\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0$) as follows:

$$
\begin{aligned}
&(a \bigotimes b) \ mod \ p(x) = (\alpha \bigotimes b) \ mod \ p(x) \\
&= (b_3\alpha^4 + b_2\alpha^3 + b_1\alpha^2 + b_0\alpha) \ mod \ p(x) \\
&= (b_2\alpha^3 + b_1\alpha^2 + (b_3 + b_0)\alpha + b_3) \ mod \ p(x)
\end{aligned}
$$

which corresponds to the 4×4 corresponding multiplication binary matrix of the finite field element $\alpha \in \mathbb{F}_{2^4}/$`0x13` as follows:

$$
\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}
$$

Then, XOR (α) is obtained as $1 (= 5 - 4)$ since Hamming weight of the 4×4 binary matrix is 5.

Definition 2 ([9]): s- XOR (a) is defined as the minimum number of XORs needed to implement the $m \times m$ multiplication binary matrix after performing a sequence of XOR operations.

Local and global optimization techniques are the two different techniques to optimize MDS matrices in view of the required number of XOR operations. In local optimization, every element of a $k \times k$ matrix over $\mathbb{F}_{2^m}$ is considered, whereas, in global optimization a $k \times k$ matrix over $\mathbb{F}_{2^m}$ is first transformed into its corresponding $mk \times mk$ binary matrix and then this binary matrix is optimized. Global optimization techniques can be grouped into two main approaches: cancelation-free programs and heuristic. In cancelation-free programs, the required number of XORs for a matrix is reduced by eliminating common sub-expressions iteratively. Shortest Linear Programs (SLP) [17] for MDS matrices are in the category of global optimization techniques and use heuristic. In this paper, we use a heuristic algorithm, namely Boyar-Peralta algorithm [18], [17] (shortly BP), to optimize MDS matrices and compare them with the ones given in the literature.

3. Our approach for generating MDS matrices

In this paper, we follow the idea given in [9] and [14] to generate new MDS matrices for lightweight cryptography. This idea is based on the application of some new parameters (d_is) to MDS matrices, which provides to keep both MDS and involutory properties of these matrices. By using the idea, we generate new MDS matrices, which have low XOR counts. In this context, first, we generate new MDS matrices by considering low naive XOR counts. Then, we optimize these matrices and find MDS matrices with the lowest XOR counts. In [9] and [14], the idea was used only for 3×3 involutory matrices and Hadamard matrices (4×4 and 8×8 matrices) to generate involutory/non-involutory MDS matrices. In these papers, the results were obtained by evaluating these matrices in view of naive XOR count. In addition to Hadamard matrices, one can also use circulant and Toeplitz matrices [22] to generate MDS matrices by search. By using our approach, we aim to apply the idea to circulant and Toeplitz matrices to generate MDS matrices with the lowest XOR counts (to the best our knowledge). In Theorem 1, the idea preserving both MDS and involutory properties for 2×2 matrices is given. It can easily be proven that the idea is applicable to any $k \times k$ MDS matrix.

Theorem 1: Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ be any 2×2 matrix over $\mathbb{F}_{2^m}$. If the matrix A is involutory and MDS, then there exists an element d_0 such that $a_{11} = a_{22}$, $a_{12} = (a_{11} + 1)d_0$, $a_{21} = (a_{11} + 1){d_0}^{-1}$. Hence, the matrix form to generate all 2×2 involutory MDS matrices can be expressed as:

$$IM_{2\times2}(a_{11}, d_0) = \begin{bmatrix} a_{11} & (a_{11}+1)d_0 \\ (a_{11}+1){d_0}^{-1} & a_{11} \end{bmatrix}$$

where $d_0 \in \mathbb{F}_{2^m} - \{0\}$ and $a_{11} \in \mathbb{F}_{2^m} - \{0, 1\}$. Then, the number of all 2×2 involutory MDS matrices over $\mathbb{F}_{2^m}$ is $(2^m - 2) \cdot (2^m - 1)$.

Proof: Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ be any 2×2 involutory matrix with $a_{11} \neq 0$. Let c_{ij} denote elements of A^2 for $i, j \in \{1, 2\}$, i.e., $c_{ij} = \sum_{k=1}^{2} a_{ik}a_{kj}$. Since $A^2 = I$, if $i = j$ then $c_{ij} = 1$ and if $i \neq j$ then $c_{ij} = 0$, we get the following equations:

$$a_{11}^2 + a_{12}a_{21} = 1 \quad (1)$$
$$a_{11}a_{12} + a_{12}a_{22} = 0 \quad (2)$$
$$a_{21}a_{11} + a_{22}a_{21} = 0 \quad (3)$$
$$a_{21}a_{12} + a_{22}^2 = 1 \quad (4)$$

By adding the equations (1) and (4) given above, we have $a_{11}^2 = a_{22}^2$. Since the operations are performed in the finite field $\mathbb{F}_{2^m}$, the equality $a_{11}^2 = a_{22}^2$ can be rewritten as $(a_{11} + a_{22})^2 = 0$. Therefore, $a_{11} = a_{22}$. Moreover, from the equation (1), we have $a_{12}a_{21} = a_{11}^2 + 1 = (a_{11} + 1)^2$. Then, there exists an element $d_0 \in \mathbb{F}_{2^m} - \{0\}$ such that $a_{12} = (1 + a_{11})d_0$ and $a_{21} = (1 + a_{11}){d_0}^{-1}$. In order to have a 2×2 MDS matrix form (in addition to involutory property), the determinant of the 2×2 matrix form should be different from 0 by property 1 for MDS matrices. Then, we have the restrictions for the 2×2 matrix form as follows: $d_0 \in \mathbb{F}_{2^m} - \{0\}$ and $a_{11} \in \mathbb{F}_{2^m} - \{0, 1\}$. Hence, by using the 2×2 matrix form and the given restrictions, we obtain the number of all 2×2 involutory and MDS matrices over $\mathbb{F}_{2^m}$ as $(2^m - 2) \cdot (2^m - 1)$.

□

Theorem 1 states that all 2×2 involutory MDS matrices can easily be generated by using the given matrix form $IM_{2\times2}(a_{11}, d_0)$ and any 2×2 involutory MDS matrix belongs to a class. If one generates the representative matrices for each class, then other in-

volutory MDS matrices can be generated easily (by using the parameters d_is). Hence, one can search for better 2×2 involutory and MDS matrices from viewpoint of XOR count after optimizing them. The 2×2 matrix form $IM_{2\times2}(a_{11}) = \begin{bmatrix} a_{11} & a_{11}+1 \\ a_{11}+1 & a_{11} \end{bmatrix}$ with the given restrictions is the representative matrix form and can be used to generate all 2×2 involutory and MDS representative matrices. This representative matrix form is also a 2×2 Hadamard matrix, where XOR sum of the elements of each row and each column equals to 1.

As given in [9], one can also prove the existence of the parameters d_0 and d_0^{-1} in the matrix form $IM_{2\times2}(a_{11}, d_0)$ by applying a special combination of both multiplication of rows and columns by any non-zero element of $\mathbb{F}_{2^m}$ to $IM_{2\times2}(a_{11}) = \begin{bmatrix} a_{11} & a_{11}+1 \\ a_{11}+1 & a_{11} \end{bmatrix}$, which also preserve the MDS property of a given matrix. In this paper, we apply these parameters preserving both involutory and MDS property to 4×4 Hadamard, circulant and Toeplitz matrices to generate new MDS matrices with low XOR counts. Then, we optimize these matrices to generate the lightest ones in the literature.

A 4×4 Hadamard matrix form $H = had(a_0, a_1, a_2, a_3)$ can be given as follows:

$$H = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix}.$$

In this respect, a 4×4 Hadamard matrix with 3 more parameters (d_1, d_2, d_3 and their inverses) called Generalized Hadamard (GHadamard) matrix form $Ghad(a_0, a_1; b_1, a_2; b_2, a_3; b_3)$ can be defined as follows [14]:

$$GH = \begin{bmatrix} a_0 & a_1d_1 & a_2d_2 & a_3d_3 \\ a_1d_1^{-1} & a_0 & a_3d_1^{-1}d_2 & a_2d_1^{-1}d_3 \\ a_2d_2^{-1} & a_3d_2^{-1}d_1 & a_0 & a_1d_2^{-1}d_3 \\ a_3d_3^{-1} & a_2d_3^{-1}d_1 & a_1d_3^{-1}d_2 & a_0 \end{bmatrix}.$$

A 4×4 circulant matrix form $C = circ(a_0, a_1, a_2, a_3)$ can be given as follows:

$$C = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_3 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_0 \end{bmatrix}.$$

In this respect, a 4×4 circulant matrix form with 3 more parameters (d_1, d_2, d_3 and their inverses) $CP(a_0, a_1; d_1, a_2; d_2, a_3; d_3)$ can be defined as follows:

$$CP = \begin{bmatrix} a_0 & a_1d_1 & a_2d_2 & a_3d_3 \\ a_3d_1^{-1} & a_0 & a_1d_1^{-1}d_2 & a_2d_1^{-1}d_3 \\ a_2d_2^{-1} & a_3d_2^{-1}d_1 & a_0 & a_1d_2^{-1}d_3 \\ a_1d_3^{-1} & a_2d_3^{-1}d_1 & a_3d_3^{-1}d_2 & a_0 \end{bmatrix}.$$

A 4×4 Toeplitz matrix form with seven parameters $T = Toep(a_0, a_1, a_2, a_3, a_4, a_5, a_6)$ can be given as follows:

$$T = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_0 & a_1 & a_2 \\ a_5 & a_4 & a_0 & a_1 \\ a_6 & a_5 & a_3 & a_0 \end{bmatrix}.$$

In this respect, a 4×4 Toeplitz matrix form with 3 more parameters (d_1, d_2, d_3 and their inverses) $TP = Toep(a_0, a_1; d_1, a_2; d_2, a_3; d_3, a_4, a_5, a_6)$ can be defined as follows:

$$TP = \begin{bmatrix} a_0 & a_1d_1 & a_2d_2 & a_3d_3 \\ a_4d_1^{-1} & a_0 & a_1d_1^{-1}d_2 & a_2d_1^{-1}d_3 \\ a_5d_2^{-1} & a_4d_2^{-1}d_1 & a_0 & a_1d_2^{-1}d_3 \\ a_6d_3^{-1} & a_5d_3^{-1}d_1 & a_4d_3^{-1}d_2 & a_0 \end{bmatrix}.$$

In this paper, first, we obtain 4×4 involutory/noninvolutory MDS matrices by search and using the matrix forms Hadamard, circulant and Toeplitz (namely H, C and T, respectively). Then, we generate new MDS matrices directly by using the new forms defined (namely GH, CP and TP, respectively). Note that involutory matrices can only be obtained by using both Hadamard and GHadamard matrix forms satisfying the condition $\sum_{k=0}^{3} a_k = 1$ since we are in $\mathbb{F}_2$.

4. Experimental results for lightweight matrices

In this paper, we generate MDS matrices by using the defined forms in Section 3. By the defined forms, one can generate totally $3375(= 15^3)$ 4×4 MDS matrices from one 4×4 MDS matrix over $\mathbb{F}_{2^4}$ because these forms include additional 3 more parameters/finite field elements of $\mathbb{F}_{2^4} - \{0\}$ (namely d_1, d_2 and d_3) preserving the MDS property (and also involutory property) of a given MDS matrix. That means one can generate a huge amount of MDS matrices that should be optimized by using SLP. Therefore, we have identified a threshold based on naive XOR counts MDS matrices have. In the literature, it is known that the best naive XOR counts are 64 [14] and 58 [22] for 4×4 involutory and noninvolutory MDS matrices, respectively. In this context, we generated MDS matrices with naive XOR counts between 64 and 80 for involutory MDS matrices and naive XOR counts between 58 and 80 for involutory MDS matrices (up to 80 for GHadamard matrix type, up to 79 for circulant matrices with 3 more parameters and up to 62 by fixing the first element a_0 to 1 for Toeplitz matrices with 3 more parameters). Then, we optimized these matrices by using BP. We present one of the lightest MDS matrices for each form in the Examples below. Nevertheless, MDS matrices with better XOR counts after optimizing may be obtained by searching through all candidates. In Example 2, we present a 4×4 involutory MDS matrix (GHadamard) with the naive XOR count 68. This matrix can be implemented by 39 XORs after optimizing with BP.

Example 2: Let $\mathbb{F}_{2^4}$ be generated by the primitive element α which is a root of the primitive polynomial $x^4 + x + 1$ (`0x13`). Consider the 4×4 Hadamard and involutory MDS matrix $H_1 = had(\texttt{0x1}, \texttt{0x2}, \texttt{0x5}, \texttt{0x7}) = had(1, \alpha, \alpha^8, \alpha^{10})$

$$H_1 = \begin{bmatrix} 1 & \alpha & \alpha^8 & \alpha^{10} \\ \alpha & 1 & \alpha^{10} & \alpha^8 \\ \alpha^8 & \alpha^{10} & 1 & \alpha \\ \alpha^{10} & \alpha^8 & \alpha & 1 \end{bmatrix}$$

over $\mathbb{F}_{2^4}/\texttt{0x13}$. Then, GHadamard matrix $GH_1 = Ghad(1, \alpha; \alpha^2, \alpha^8; \alpha^7, \alpha^{10}; \alpha^8)$ corresponding to H_1 with the parameters $d_1 = \alpha^2$, $d_2 = \alpha^7$ and $d_3 = \alpha^8$ is given below:

$$GH_1 = \begin{bmatrix} 1 & \alpha^3 & 1 & \alpha^3 \\ \alpha^{14} & 1 & 1 & \alpha^{14} \\ \alpha & \alpha^5 & 1 & \alpha^2 \\ \alpha^2 & \alpha^2 & 1 & 1 \end{bmatrix}$$

which is a 4×4 involutory and MDS matrix with naive XOR count 68 and can be implemented by 39 XORs after using optimization technique BP (See Appendix).

In Example 3, we present a 4×4 non-involutory MDS matrix (GHadamard) with naive XOR count

80. This matrix can be implemented by 38 XORs after optimizing with BP.

Example 3: Let $\mathbb{F}_{2^4}$ be generated by the primitive element α which is a root of the primitive polynomial x^4+x+1 (0x13). Consider the 4×4 Hadamard MDS matrix $H_2 = had(\texttt{0x1}, \texttt{0x4}, \texttt{0x6}, \texttt{0x9}) = had(1, \alpha^2, \alpha^5, \alpha^{14})$

$$H_2 = \begin{bmatrix} 1 & \alpha^2 & \alpha^5 & \alpha^{14} \\ \alpha^2 & 1 & \alpha^{14} & \alpha^5 \\ \alpha^5 & \alpha^{14} & 1 & \alpha^2 \\ \alpha^{14} & \alpha^5 & \alpha^2 & 1 \end{bmatrix}$$

over $\mathbb{F}_{2^4}/\texttt{0x13}$. Then, GHadamard matrix $GH_2 = Ghad(1, \alpha^2; \alpha^2, \alpha^5; \alpha^2, \alpha^{14}; 1)$ corresponding to H_2 with the parameters $d_1 = \alpha^2$, $d_2 = \alpha^2$ and $d_3 = 1$ is given below:

$$GH_2 = \begin{bmatrix} 1 & \alpha^4 & \alpha^7 & \alpha^{14} \\ 1 & 1 & \alpha^{14} & \alpha^3 \\ \alpha^3 & \alpha^{14} & 1 & 1 \\ \alpha^{14} & \alpha^7 & \alpha^4 & 1 \end{bmatrix}$$

which is a 4×4 involutory and MDS matrix with naive XOR count 80 and can be implemented by 38 XORs after optimizing with BP.

In Example 4, we present a 4×4 Toeplitz MDS matrix with 3 more parameters and naive XOR count 62. This matrix can be implemented by 38 XORs after optimizing with BP.

Example 4: Let $\mathbb{F}_{2^4}$ be generated by the primitive element α which is a root of the primitive polynomial $x^4 + x + 1$ (0x13). Consider the 4×4 Toeplitz MDS matrix $T_1 = Toep(\texttt{0x1}, \texttt{0x1}, \texttt{0x6}, \texttt{0x3}, \texttt{0xd}, \texttt{0xf}, \texttt{0xa}) = Toep(1, 1, \alpha^5, \alpha^4, \alpha^{13}, \alpha^{12}, \alpha^9)$

$$T_1 = \begin{bmatrix} 1 & 1 & \alpha^5 & \alpha^4 \\ \alpha^{13} & 1 & 1 & \alpha^5 \\ \alpha^{12} & \alpha^{13} & 1 & 1 \\ \alpha^9 & \alpha^{12} & \alpha^{13} & 1 \end{bmatrix}$$

over $\mathbb{F}_{2^4}/\texttt{0x13}$. Then, the Toeplitz matrix T_1 with the parameters $d_1 = \alpha^{13}$, $d_2 = \alpha^{12}$ and $d_3 = \alpha^{10}$ $TP_1 = Toep(1, 1; \alpha^{13}, \alpha^5; \alpha^{12}, \alpha^4; \alpha^{10}, \alpha^{13}, \alpha^{12}, \alpha^9)$ corresponding to T_1 is given below:

$$TP_1 = \begin{bmatrix} 1 & \alpha^{13} & \alpha^2 & \alpha^{14} \\ 1 & 1 & \alpha^{14} & \alpha^2 \\ 1 & \alpha^{14} & 1 & \alpha^{13} \\ \alpha^{14} & 1 & 1 & 1 \end{bmatrix}.$$

which is a 4×4 MDS matrix with naive XOR count 62 and can be implemented by 38 XORs after using optimization technique BP.

In Example 5, we present a 4×4 circulant MDS matrix with 3 more parameters and naive XOR count 74. This matrix can be implemented by 38 XORs after optimizing with BP.

Example 5: Let $\mathbb{F}_{2^4}$ be generated by the primitive element α which is a root of the primitive polynomial $x^4 + x + 1$ (0x13). Consider the 4×4 circulant MDS matrix $C_1 = circ(\texttt{0x1}, \texttt{0xe}, \texttt{0x2}, \texttt{0xa}) = circ(1, \alpha^{11}, \alpha, \alpha^9)$

$$C_1 = \begin{bmatrix} 1 & \alpha^{11} & \alpha & \alpha^9 \\ \alpha^9 & 1 & \alpha^{11} & \alpha \\ \alpha & \alpha^9 & 1 & \alpha^{11} \\ \alpha^{11} & \alpha & \alpha^9 & 1 \end{bmatrix}$$

over $\mathbb{F}_{2^4}/\texttt{0x13}$. Then, the circulant matrix C_1 with the parameters $d_1 = \alpha^7$, $d_2 = 1$ and $d_3 = \alpha^8$ $CP_1 = CP(1, \alpha^{11}; \alpha^7, \alpha; 1, \alpha^9; \alpha^8)$ corresponding to C_1 is given below:

$$CP_1 = \begin{bmatrix} 1 & \alpha^3 & \alpha & \alpha^2 \\ \alpha^2 & 1 & \alpha^4 & \alpha^2 \\ \alpha & \alpha & 1 & \alpha^4 \\ \alpha^3 & 1 & \alpha & 1 \end{bmatrix}.$$

which is a 4×4 MDS matrix with naive XOR count 74 and can be implemented by 38 XORs after using optimization technique BP.

Table 1
Comparision of XOR counts for matrices available in the literature

4×4 Matrix over $\mathbb{F}_{2^4}$	Type	XOR count optimized with BP
[12]	Hadamard	48 (given in [17])
[23]	Circulant	44 (given in [17])
[24]	Circulant	42 (given in [17])
[22]	Toeplitz	43 (given in [17])
[20]		43 (given in [17])
[12]	Hadamard (involutory)	48 (given in [17])
[22]	Involutory	42 (given in [17])
[20]	Involutory	47 (given in [17])
Example 2	GHadamard (involutory)	39
Example 3	GHadamard	38
Example 4	TP	38
Example 5	CP	38

In Table 1, we compare our results with available matrices in the literature after optimizing with BP given in [17]. The results show that our methods can be used to generate 4×4 involutory/non-involutory MDS matrices with good implementation properties in view of XOR count.

5. Conclusion

In this paper, we obtained the lightest 4×4 involutory/non-involutory MDS matrices (to the best of our knowledge) in view of XOR count after optimizing with BP by applying the idea given in [9] and [14] to some special matrix forms such as 4×4 Hadamard, circulant and Toeplitz matrix forms. In [9], a direct construction method was given to generate all 3×3 involutory and MDS matrices, which uses 2 more parameters (because of the dimension) applied to a 3×3 matrix form that is basis matrix form and can be considered as a representative matrix form. In the future, we will concentrate on developing a new hybrid construction method to generate all 4×4 involutory and MDS matrices over $\mathbb{F}_{2^m}$ and try to find better matrices in view of XOR count after optimizing with BP than the matrices given in this paper.

By using the methods presented in this paper, one can generate 4×4 MDS matrices with good implementation properties easily. Moreover, these methods can also be applied to generate 4×4 involutory/non-involutory MDS matrices over $\mathbb{F}_{2^8}$. But, we have not obtained MDS matrices over $\mathbb{F}_{2^8}$ because the presented methods generate a huge amount of MDS matrices that should be evaluated in view of XOR count after optimizing with BP. In the future, we will focus on a more clever method to find lightweight MDS matrices over $\mathbb{F}_{2^8}$ (also by using methods presented in this paper) after optimizing with BP. Finally, the methods presented here are generic and the ideas can easily be applied to any $k \times k$ MDS matrices to generate new lightweight MDS matrices.

Acknowledgment

The authors would like to thank to the anonymous reviewers of the IJISS and Assoc. Prof. Dr. Sedat Akleylek for their valuable comments, which have

enhanced the quality of the paper. Meltem Kurt Pehlivanoğlu is partially supported by TÜBİTAK under 2219-Postdoctoral Research Program Grant.

Appendix

The appendix presents the optimization result of 4×4 involutory MDS matrix GH_1 over $\mathbb{F}_{2^4}$, where $[x_0, x_1, \ldots, x_{15}]$, $[y_0, y_1, \ldots, y_{15}]$ and t_is represent input bits, output bits and temporary variables, respectively.

$$
\begin{aligned}
t_0 &= x_2 + x_6 & y_{14} &= t_{15} + t_{18} \\
t_1 &= x_3 + x_7 & t_{21} &= t_1 + t_3 \\
t_2 &= x_5 + x_{13} & y_6 &= t_{18} + t_{21} \\
t_3 &= x_6 + x_{14} & y_8 &= x_8 + t_{21} \\
t_4 &= x_9 + t_3 & t_{24} &= x_{13} + t_4 \\
t_5 &= x_0 + x_4 & y_1 &= t_{10} + t_{24} \\
t_6 &= x_{10} + x_{15} & t_{26} &= t_0 + t_2 \\
t_7 &= x_8 + x_{12} & y_5 &= t_{24} + t_{26} \\
y_{12} &= t_0 + t_7 & y_{11} &= x_{11} + t_{26} \\
t_9 &= x_{11} + x_{12} & t_{29} &= x_0 + x_8 \\
t_{10} &= x_1 + x_5 & y_0 &= t_2 + t_{29} \\
t_{11} &= x_7 + t_6 & t_{31} &= x_4 + x_{12} \\
t_{12} &= x_0 + x_7 & t_{32} &= t_{10} + t_{31} \\
y_7 &= t_9 + t_{12} & y_4 &= y_0 + t_{32} \\
t_{14} &= x_3 + x_{15} & y_{10} &= t_{11} + t_{32} \\
t_{15} &= t_5 + t_{14} & t_{35} &= x_{11} + x_{15} \\
y_3 &= y_7 + t_{15} & y_{15} &= t_{10} + t_{35} \\
y_9 &= t_4 + t_{15} & t_{37} &= t_0 + t_{21} \\
t_{18} &= x_{14} + t_{11} & y_{13} &= t_{24} + t_{37} \\
y_2 &= t_0 + t_{18}
\end{aligned}
$$

References

[1] C.E. Shannon."Communication Theory of Secrecy Systems", *Bell System Technical Journal*, Vol.28, pp. 656-715, October 1949.

[2] E. Biham, A. Shamir. "Differential cryptanalysis of DES-like cryptosystems", *CRYPTO'90*, Santa Barbara, CA, USA, LNCS, Vol.537, pp. 2-21, 11-15 August 1990.

[3] M. Matsui. "Linear cryptanalysis method for DES cipher", *EUROCRYPT'93*, Lofthus, Norway, LNCS, Vol.765, pp. 386-397, 23-27 May 1993.

[4] A.M. Youssef, S. Mister, S.E. Tavares. "On the Design of Linear Transformation for Substitution Permutation Encryption Networks", *Selected Areas in Cryptography (SAC)*, Ottawa Ontario, Canada, pp. 40-48, 11-12 August 1997.

[5] J. Guo, T. Peyrin, A. Poschmann. "The PHOTON family of lightweight hash functions", *CRYPTO 2011*, Santa Barbara, CA, USA, LNCS, Vol.6841, pp. 222-239, 14-18 August 2011.

[6] K.C. Gupta, I.G. Ray. "On constructions of MDS matrices from companion matrices for lightweight cryptography", *CD-ARES 2013*, Regensburg, Germany, LNCS, Vol.8128, pp. 29-43, 2-6 September 2013.

[7] J. Lacan, J. Fimes. "Systematic MDS erasure codes based on vandermonde matrices", *IEEE Communications Letters*, Vol.8, No.9, pp. 570-572, September 2004.

[8] 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, No.3, pp.287-308, September 2012.

[9] G.G. Güzel, M.T. Sakallı, S. Akleylek, V. Rijmen, Y. Çengellenmiş. "A New Matrix Form to Generate All 3×3 Involutory MDS Matrices over $\mathbb{F}_{2^m}$", *Information Processing Letters*, Vol.147, pp. 61-68, March 2019.

[10] M. Sajadieh, M. Dakhilalian, H. Mala, P. Sepehrdad. "Recursive Diffusion Layers for Block Ciphers and Hash Functions", *FSE 2012*, Washington DC, USA, LNCS, Vol.7549, pp. 385-401, 19-21 March 2012.

[11] S. Wu, M. Wang, W. Wu. "Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions", *Selected Areas in Cryptography (SAC)*, Windsor, ON, Canada, LNCS, Vol.7707, pp. 355-371, 15-16 August 2012.

[12] S.M. Sim, K. Khoo, F. Oggier, T. Peyrin. "Lightweight MDS Involution Matrices", *FSE 2015*, Istanbul, Turkey, LNCS, Vol.9054, pp. 471-493, 8-11 March 2015.

[13] S. Akleylek, M.T. Sakallı. "Some Results on MDS Matrices", *9th International Conference on Information Security and Cryptology (ISCTURKEY 2016)*, Ankara, Turkey, pp. 35-38, 25-26 October 2016.

[14] M.K. Pehlivanoğlu, M.T. Sakallı, S. Akleylek, N. Duru, V. Rijmen. "Generalisation of Hadamard Matrix to Generate Involutory MDS Matrices for Lightweight Cryptography", *IET Information Security*, Vol.12, No.4, pp. 348-355, July 2018.

[15] M.T. Sakallı, S. Akleylek, K. Akkanat, V. Rijmen. "On the automorphisms and isomorphisms of MDS matrices and their efficient implementations", *Turkish Journal of Electrical & Computer Sciences*, Vol.28, No. 1, pp. 275-287, January 2020.

[16] K. Khoo, T. Peyrin, A.Y. Poschmann, and H. Yap. "FOAM: Searching for Hardware-Optimal SPN Structures and Compo-

nents with a Fair Comparison", *CHES 2014*, Busan, South Korea, LNCS, Vol.8731, pp. 433-450, 23-26 September 2014.

[17] T. Kranz, G. Leander, K. Stoffelen, and F. Wiemer. "Shorter linear straight-line programs for MDS matrices", *IACR Transactions on Symmetric Cryptology*, Vol.2017, No.4, pp. 188-211, December 2017.

[18] J. Boyar, R. Peralta. "A new combinational logic minimization technique with applications to cryptology", *SEA 2010*, Naples, Italy, LNCS, vol. 6049, pp. 178–189, 20-22 May 2010.

[19] F.J. MacWilliams, N.J.A. Sloane. *The theory of error-correcting codes*. North-Holland, Amsterdam:North Holland Publishing Co., 1977.

[20] J. Jean, T. Peyrin, S.M. Sim, J. Tourteaux. "Optimizing implementations of lightweight building blocks", *IACR Transactions on Symmetric Cryptology*, Vol.2017, No.4, pp. 130-168, December 2017.

[21] C. Beierle, T. Kranz, G. Leander. "Lightweight multiplication in $GF(2^n)$ with applications to MDS matrices", *CRYPTO 2016*, Santa Barbara, USA, LNCS, vol. 9814, pp. 625-653, 14-18 August 2016.

[22] S. Sarkar, H. Syed. "Lighweight diffusion layer: importance of Toeplitz matrices", *IACR Transactions on Symmetric Cryptology*, Vol.2016, No.1, pp. 95-113, January 2016.

[23] M. Liu, S.M. Sim. "Lightweight MDS generalized circulant matrices", *FSE 2016*, Bochum, Germany, LNCS, Vol. 9783, pp. 101–120, 20-23 March 2016.

[24] Y. Li, M. Wang. "On the construction of lightweight circulant involutory MDS matrices", *FSE 2016*, Bochum, Germany, LNCS, Vol. 9783, pp. 121–139, 20-23 March 2016.