On Involutory MDS Matrices over Binary Field Extensions [1]

Muharrem Tolga Sakallı

Department of Computer Engineering, Trakya University, Edirne, Turkey

tolga@trakya.edu.tr

December 3, 2019

[1] This presentation includes many parts from published/unpublished/submitted joint works with Sedat Akleylek, Vincent Rijmen, Meltem Kurt Pehlivanoğlu, G. Gözde Güzel, Kemal Akkanat, Nevcihan Duru, Yasemin Çengellenmiş, Fatma B. Sakallı.

Outline

- On constructions of (involutory) MDS matrices in the literature
- A matrix form to generate all 2×2 involutory MDS matrices
- Generalization of Hadamard Matrix to generate (involutory) MDS matrices (published results)
- A new matrix form to generate all 3×3 involutory MDS matrices (published results)
- How to generate all 4×4 involutory MDS matrices over binary field extensions (unpublished results)
- Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$ (accepted)
- Conclusions

On constructions of (involutory) MDS matrices in the literature

- 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.
- 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.

On constructions of (involutory) MDS matrices in the literature

MDS matrices have the maximum differential and linear branch number ($k+1$ for $k \times k$ MDS matrices). Some important properties of MDS matrices can be given as follows:

- A square matrix A is MDS if and only if every square submatrix of A is nonsingular.
- 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 [1].
- The MDS property of a matrix is preserved under the transpose operation [1].

On constructions of (involutory) MDS matrices in the literature

- In the literature, there are several construction methods of MDS matrices as follows:
  - Direct construction methods like Cauchy matrices [2] and Vandermonde matrices [3, 4].
  - Search based methods by using some special matrix forms like circulant matrices, Finite Field Hadamard matrices (shortly Hadamard matrices) and Toeplitz matrices [5].
  - Subfield construction [6, 7].

On constructions of (involutory) MDS matrices in the literature

- In this presentation, new three construction types (methods)
  - a new hybrid construction method focusing on generating (involutory) MDS matrices (Generalized Hadamard Matrix [8])
  - a new direct construction method focusing on generating all 3×3 involutory MDS matrices [9]
  - a new construction method (based on clever search) focusing on generating all 4×4 involutory MDS matrices.

  will be introduced.

On constructions of (involutory) MDS matrices in the literature

- A direct construction method focusing on generating all 3×3 involutory MDS matrices is based on a new matrix form.
- A new construction method focusing on generating all 4×4 involutory MDS matrices is based on the idea that any involutory matrix belongs to a class. This idea is closely related with that of Generalized Hadamard matrix form (GHadamard).
- In this context, the definition of Hadamard matrix is modified.

A matrix form to generate all 2×2 involutory MDS matrices

Theorem

Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ *be a* 2×2 *matrix over* $\mathbb{F}_{2^m}$ *If the matrix* A *is involutory MDS, then there exists an element* b_0 *such that* $a_{11} = a_{22}$, $a_{12} = (a_{11} + 1)b_0$, $a_{21} = (a_{11} + 1){b_0}^{-1}$. *Hence, the matrix form to generate all* 2×2 *involutory MDS matrices can be expressed as:*

$$IM_{2\times 2}(a_{11}, b_0) = \begin{bmatrix} a_{11} & (a_{11}+1)b_0 \\ (a_{11}+1){b_0}^{-1} & a_{11} \end{bmatrix}$$

where $b_0 \in \mathbb{F}_{2^m} - \{0\}$ *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* $(2^m - 2) \cdot (2^m - 1)$.

A matrix form to generate all 2×2 involutory MDS matrices

Proof.

Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ be 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:

$$\begin{aligned} a_{11}^2 + a_{12}a_{21} &= 1 \\ a_{11}a_{12} + a_{12}a_{22} &= 0 \\ a_{21}a_{11} + a_{22}a_{21} &= 0 \\ a_{21}a_{12} + a_{22}^2 &= 1 \end{aligned}$$

$\square$

A matrix form to generate all 2×2 involutory MDS matrices

Proof.

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, $a_{11} = a_{22}$. Morever, from the equation (1), we have $a_{12}a_{21} = a_{11}^2 + 1 = (a_{11} + 1)^2$. Then, there exists an element $b_0 \in \mathbb{F}_{2^m} - \{0\}$ such that $a_{12} = (1 + a_{11})b_0$ and $a_{21} = (1 + a_{11}){b_0}^{-1}$. □

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

- Hence, we can generate all 2×2 involutory MDS matrices over $\mathbb{F}_{2^m}$ by using the matrix form

$$IM_{2\times 2}(a_{11}, b_0) = \begin{bmatrix} a_{11} & (a_{11}+1)b_0 \\ (a_{11}+1){b_0}^{-1} & a_{11} \end{bmatrix}.$$

- The determinant of the 2×2 matrix form $IM_{2\times 2}$ is different from 0 iff $a_{11} \in \mathbb{F}_{2^m} - \{0, 1\}$ and $b_0 \in \mathbb{F}_{2^m} - \{0\}$.
- We call the matrix form $IMR_{2\times 2}(a_{11})$ (not consisting of the parameter b_0 and its inverse) as representative matrix form used for obtaining representative matrices, which can be used to generate all 2×2 involutory MDS matrices:

$$IMR_{2\times 2}(a_{11}) = \begin{bmatrix} a_{11} & a_{11}+1 \\ a_{11}+1 & a_{11} \end{bmatrix}.$$

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

- Note that the representative matrix form $IMR_{2\times2}(a_{11})$ is a 2×2 Hadamard matrix. XOR sum of the elements in any row/column is equal to 1 and XOR sum of the elements in any diagonal is equal to 0.
- One can also prove the existance of the parameters b_0 and b_0^{-1} in the matrix form $IM_{2\times2}(a_{11}, b_0)$ by applying a special combination of both multiplication of rows and columns by any non-zero element of $\mathbb{F}_{2^m}$ to $IMR_{2\times2}(a_{11})$, which also preserve the MDS property of a given matrix.

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

- Consider $IMR_{2\times 2}(a_{11}) = \begin{bmatrix} a_{11} & a_{11}+1 \\ a_{11}+1 & a_{11} \end{bmatrix}$. First, multiply the first and second column of $IMR_{2\times 2}(a_{11})$ by α^{i_1} and α^{i_2} for $0 \leq i_1, i_2 \leq 2^m - 2$, respectively, where α is any primitive element of $\mathbb{F}_{2^m}$.
- Then, multiply the first and second row of $IMR_{2\times 2}(a_{11})$ by α^{-i_1} and α^{-i_2}, respectively. The resultant 2×2 matrix $IMR_{2\times 2}(a_{11})$ can be given as follows:

$$IMR_{2\times 2}(a_{11}) = \begin{bmatrix} a_{11} & (a_{11}+1)\alpha^{i_2-i_1} \\ (a_{11}+1)\alpha^{i_1-i_2} & a_{11} \end{bmatrix}.$$

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

- By substituting $\alpha^{i_2-i_1}$ and $\alpha^{i_1-i_2}$ with b_0 and b_0^{-1}, respectively, in the matrix $IMR_{2\times 2}(a_{11})$. We obtain

$$IM_{2\times 2}(a_{11}, b_0) = \begin{bmatrix} a_{11} & (a_{11}+1)b_0 \\ (a_{11}+1){b_0}^{-1} & a_{11} \end{bmatrix}.$$

- It can easily be proven that the idea can be applied to any $k \times k$ MDS matrix. If it is applied to a $k \times k$ involutory MDS matrix over $\mathbb{F}_{2^m}$, then new involutory and MDS matrices are generated. Also, one $k \times k$ involutory MDS matrix over $\mathbb{F}_{2^m}$, in fact, defines totally $(2^m - 1)^{k-1}$ involutory MDS matrices, which we call these matrices a class.

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

- If the idea is applied to a Hadamard matrix H, we obtain a new matrix form, which we call Generalized Hadamard matrix, GHadamard.
- For a Hadamard matrix H, the equality $H^2 = c^2 I$ holds, where c is a finite field element and I is the identity matrix. Then, the equality also holds for a GHadamard matrix GH i.e., $(GH)^2 = c^2 I$.
- In this respect, a 4×4 GHadamard matrix $Ghad(a_0, a_1; b_1, a_2; b_2, a_3; b_3)$ can be given as follows:

$$GH = \begin{bmatrix} a_0 & a_1 b_1 & a_2 b_2 & a_3 b_3 \\ a_1 b_1^{-1} & a_0 & a_3 b_1^{-1} b_2 & a_2 b_1^{-1} b_3 \\ a_2 b_2^{-1} & a_3 b_2^{-1} b_1 & a_0 & a_1 b_2^{-1} b_3 \\ a_3 b_3^{-1} & a_2 b_3^{-1} b_1 & a_1 b_3^{-1} b_2 & a_0 \end{bmatrix}.$$

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

- Similarly, one can easily obtain an 8×8 GHadamard matrix $Ghad(a_0, a_1; b_1, a_2; b_2, a_3; b_3, a_4; b_4, a_5; b_5, a_6; b_6, a_7; b_7)$ as follows:

$$GH = \begin{bmatrix} a_0 & a_1 b_1 & a_2 b_2 & a_3 b_3 & a_4 b_4 & a_5 b_5 & a_6 b_6 & a_7 b_7 \\ a_1 b_1^{-1} & a_0 & a_3 b_1^{-1} b_2 & a_2 b_1^{-1} b_3 & a_5 b_1^{-1} b_4 & a_4 b_1^{-1} b_5 & a_7 b_1^{-1} b_6 & a_6 b_1^{-1} b_7 \\ a_2 b_2^{-1} & a_3 b_2^{-1} b_1 & a_0 & a_1 b_2^{-1} b_3 & a_6 b_2^{-1} b_4 & a_7 b_2^{-1} b_5 & a_4 b_2^{-1} b_6 & a_5 b_2^{-1} b_7 \\ a_3 b_3^{-1} & a_2 b_3^{-1} b_1 & a_1 b_3^{-1} b_2 & a_0 & a_7 b_3^{-1} b_4 & a_6 b_3^{-1} b_5 & a_5 b_3^{-1} b_6 & a_4 b_3^{-1} b_7 \\ a_4 b_4^{-1} & a_5 b_4^{-1} b_1 & a_6 b_4^{-1} b_2 & a_7 b_4^{-1} b_3 & a_0 & a_1 b_4^{-1} b_5 & a_2 b_4^{-1} b_6 & a_3 b_4^{-1} b_7 \\ a_5 b_5^{-1} & a_4 b_5^{-1} b_1 & a_7 b_5^{-1} b_2 & a_6 b_5^{-1} b_3 & a_1 b_5^{-1} b_4 & a_0 & a_3 b_5^{-1} b_6 & a_2 b_5^{-1} b_7 \\ a_6 b_6^{-1} & a_7 b_6^{-1} b_1 & a_4 b_6^{-1} b_2 & a_5 b_6^{-1} b_3 & a_2 b_6^{-1} b_4 & a_3 b_6^{-1} b_5 & a_0 & a_1 b_6^{-1} b_7 \\ a_7 b_7^{-1} & a_6 b_7^{-1} b_1 & a_5 b_7^{-1} b_2 & a_4 b_7^{-1} b_3 & a_3 b_7^{-1} b_4 & a_2 b_7^{-1} b_5 & a_1 b_7^{-1} b_6 & a_0 \end{bmatrix}$$

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

Example

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

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

over $\mathbb{F}_{2^4}/\texttt{0x13}$. Then, GHadamard matrix $GH_1 = Ghad(1, \alpha^8; \alpha^7, \alpha; \alpha^{14}, \alpha^{10}; \alpha^7)$ corresponding to H_1 with the parameters $b_1 = \alpha^7$, $b_2 = \alpha^{14}$ and $b_3 = \alpha^7$ is given below:

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

Example

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

which is involutory MDS matrix with the least naive XOR count 64 $(= 16 + 4 \cdot 3 \cdot 4)$. Note that XOR count is a metric used in the estimation of hardware implementation cost. The XOR count value given is a naive result. This matrix can be implemented by 39 XORs after using optimization technique SLP (Shortest Linear Program).

SLP result for GH_1

```
t0 = x3 + x10
t1 = x5 + x15
t2 = x1 + x7
t3 = x2 + x9
t4 = x4 + x14
t5 = x3 + x11
t6 = x7 + x13
y3 = t5 + t6
t8 = x0 + x6
t9 = x8 + t2
y12 = x12 + t9
t11 = x3 + x6
t12 = x15 + t0
y4 = x4 + t12
t14 = x2 + t1
y8 = x8 + t14
t16 = x14 + t3
y7 = x7 + t16
t18 = x1 + t16
y1 = t14 + t18
t20 = x12 + t11
t21 = t0 + t8
y10 = t6 + t21
t23 = t1 + t20
y9 = t3 + t23
t25 = t5 + t21
y5 = t23 + t25
y15 = t12 + t25
t28 = t12 + t14
y2 = t23 + t28
y14 = x14 + t28
t31 = x0 + x8
y0 = t4 + t31
t33 = x11 + t2
y11 = t4 + t33
t35 = t4 + t6
y13 = t18 + t35
t37 = y3 + t9
y6 = t11 + t37
```

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

Example

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 8×8 Hadamard involutory MDS matrix $H_2 = had(\texttt{0x2}, \texttt{0xf}, \texttt{0xc}, \texttt{0x5}, \texttt{0xa}, \texttt{0x4}, \texttt{0x8}, \texttt{0x3}) = had(\alpha, \alpha^{12}, \alpha^6, \alpha^8, \alpha^9, \alpha^2, \alpha^3, \alpha^4)$ over $\mathbb{F}_{2^4}/\texttt{0x13}$.

$GH_2 = Ghad(\alpha, \alpha^{12}; \alpha^2, \alpha^6; \alpha^9, \alpha^8; \alpha^7, \alpha^9; \alpha^6, \alpha^2; \alpha^{11}, \alpha^3; \alpha^3, \alpha^4; \alpha^{13})$ corresponding to H_2 with the parameters $b_1 = \alpha^2$, $b_2 = \alpha^9$, $b_3 = \alpha^7$, $b_4 = \alpha^6$, $b_5 = \alpha^{11}$, $b_6 = \alpha^3$ and $b_7 = \alpha^{13}$ is given below:

$$GH_2 = \begin{bmatrix} \alpha & \alpha^{14} & 1 & 1 & 1 & \alpha^{13} & \alpha^6 & \alpha^2 \\ \alpha^{10} & \alpha & 1 & \alpha^{11} & \alpha^6 & \alpha^3 & \alpha^5 & \alpha^{14} \\ \alpha^{12} & \alpha & \alpha & \alpha^{10} & 1 & \alpha^6 & \alpha^3 & \alpha^6 \\ \alpha & \alpha & \alpha^{14} & \alpha & \alpha^3 & \alpha^7 & \alpha^{13} & 1 \\ \alpha^3 & \alpha^{13} & \alpha^6 & \alpha^5 & \alpha & \alpha^2 & \alpha^3 & 1 \\ \alpha^6 & 1 & \alpha^2 & \alpha^{14} & \alpha^7 & \alpha & 1 & \alpha^8 \\ 1 & \alpha^3 & 1 & \alpha^6 & \alpha^9 & \alpha & \alpha & \alpha^7 \\ \alpha^6 & \alpha^7 & \alpha^{13} & \alpha^3 & \alpha & \alpha^4 & \alpha^2 & \alpha \end{bmatrix}.$$

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

- The matrix GH_2 presented in the example is 8×8 involutory MDS matrix with the naive XOR count 407 $(= 183 + 8 \cdot 7 \cdot 4)$. This matrix can be implemented by 212 XORs after using optimization technique SLP.
- The idea can be used to generate non-involutory MDS matrices. We have generated an 8×8 non-involutory MDS matrix with the naive XOR count 380. This matrix can be implemented by 205 XORs after using optimization technique SLP.
- The idea is also appliciable to any type of $k \times k$ matrix (e.g. circulant matrices).

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

Example

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 $M_1 = circ(\mathtt{0x1}, \mathtt{0xb}, \mathtt{0x2}, \mathtt{0xa}) = circ(1, \alpha^7, \alpha, \alpha^9)$

$$M_1 = \begin{bmatrix} 1 & \alpha^7 & \alpha & \alpha^9 \\ \alpha^9 & 1 & \alpha^7 & \alpha \\ \alpha & \alpha^9 & 1 & \alpha^7 \\ \alpha^7 & \alpha & \alpha^9 & 1 \end{bmatrix}$$

over $\mathbb{F}_{2^4}/\mathtt{0x13}$. Then, $PM_1 = Pcirc(1, \alpha^7; \alpha^8, \alpha; \alpha, \alpha^9; \alpha^9)$ corresponding to M_1 with the parameters $b_1 = \alpha^8$, $b_2 = \alpha$ and $b_3 = \alpha^9$ is given below:

Generalization of Hadamard Matrix to generate (involutory) MDS matrices

Example

$$PM_1 = \begin{bmatrix} 1 & 1 & \alpha^2 & \alpha^3 \\ \alpha & 1 & 1 & \alpha^2 \\ 1 & \alpha & 1 & 1 \\ \alpha^{13} & 1 & \alpha & 1 \end{bmatrix}$$

which is non-involutory MDS matrix (including the maximum number of occurrences of 1s) with naive XOR count 61 $(= 13 + 4 \cdot 3 \cdot 4)$. This matrix can be implemented by 39 XORs after using optimization technique SLP.

A new matrix form to generate all 3×3 involutory MDS matrices

- In this section, a new matrix form to generate all 3×3 involutory MDS matrices over $\mathbb{F}_{2^m}$ is introduced. The interested reader may refer to [9] for the detailed proof on how to obtain the given form.
- The matrix form $IM_{3\times3}(a_{11}, a_{22}, b_0, b_1)$ for generating all 3×3 involutory and MDS matrices over $\mathbb{F}_{2^m}$ can be defined as follows:

$$IM_{3\times3} = \begin{bmatrix} a_{11} & (a_{11}+1)b_0 & (a_{11}+1)b_1 \\ (a_{22}+1){b_0}^{-1} & a_{22} & (a_{22}+1){b_0}^{-1}b_1 \\ (a_{11}+a_{22}){b_1}^{-1} & (a_{11}+a_{22}){b_1}^{-1}b_0 & a_{11}+a_{22}+1 \end{bmatrix}$$

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 $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$.

A new matrix form to generate all 3×3 involutory MDS matrices

- One can directly construct all 3×3 involutory MDS matrices by using 4 parameters a_{11}, a_{22}, b_0 and b_1.
- By considering the given restrictions above for a_{11}, a_{22}, b_0 and b_1, 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 $m > 2$.
- We call the matrix form $IMR_{3\times3}(a_{11}, a_{22})$ (not consisting of the parameters b_0, b_1 and their inverses) as representative matrix form used for obtaining representative matrices, which can be used to generate all 3×3 involutory MDS matrices:

$$IMR_{3\times3}(a_{11}, a_{22}) = \begin{bmatrix} a_{11} & a_{11}+1 & a_{11}+1 \\ a_{22}+1 & a_{22} & a_{22}+1 \\ a_{11}+a_{22} & a_{11}+a_{22} & a_{11}+a_{22}+1 \end{bmatrix}.$$

A new matrix form to generate all 3×3 involutory MDS matrices

- In fact, we identified 2 different representative matrix forms. The other representative matrix form is the transpose of the matrix form $IMR_{3\times3}(a_{11}, a_{22})$.
- This representative matrix form also spans all 3×3 involutory MDS matrices over $\mathbb{F}_{2^m}$ because of the parameters b_0, b_1 and their inverses. The transpose matrix form of $IMR_{3\times3}(a_{11}, a_{22})$ is as follows:

$$IMR^T_{3\times3}(a_{11}, a_{22}) = \begin{bmatrix} a_{11} & a_{22}+1 & a_{11}+a_{22} \\ a_{11}+1 & a_{22} & a_{11}+a_{22} \\ a_{11}+1 & a_{22}+1 & a_{11}+a_{22}+1 \end{bmatrix}.$$

How to generate all 4×4 involutory MDS matrices over binary field extensions

- In order to generate all 4×4 involutory MDS matrices over $\mathbb{F}_{2^m}$, first we recall the general and representative matrix form of 2×2 matrices generating all involutory and MDS matrices. These forms were as follows:

$$IM_{2\times 2}(a_{11}, b_0) = \begin{bmatrix} a_{11} & (a_{11}+1)b_0 \\ (a_{11}+1){b_0}^{-1} & a_{11} \end{bmatrix},$$

$$IMR_{2\times 2}(a_{11}) = \begin{bmatrix} a_{11} & a_{11}+1 \\ a_{11}+1 & a_{11} \end{bmatrix}.$$

How to generate all 4×4 involutory MDS matrices over binary field extensions

- Hadamard matrix form can be considered as a form generating some (involutory and MDS) representatives (which needs search to verify whether these matrices are MDS or not) that can be used to generate many involutory MDS matrices (by using the GHadamard matrix idea). But, it still does not generate all 4×4 involutory MDS matrices.
- For example, by search, one can confirm that there are 1512 4×4 involutory and MDS matrices over $\mathbb{F}_{2^4}$. Then, we recall the 4×4 Hadamard matrix form (used for generating some representative involutory MDS matrices) to be used in search as follows:

$$H = \begin{bmatrix} a & b & c & a+b+c+1 \\ b & a & a+b+c+1 & c \\ c & a+b+c+1 & a & b \\ a+b+c+1 & c & b & a \end{bmatrix}.$$

How to generate all 4×4 involutory MDS matrices over binary field extensions

- The generated 1512 4×4 involutory and MDS matrices over $\mathbb{F}_{2^4}$ are some of representative involutory and MDS matrices. In this respect, one can totally generate $1512 \cdot (2^4 - 1)^3 = 5,103,000 \approx 2^{22.28}$ involutory and MDS matrices over $\mathbb{F}_{2^4}$ by using GHadamard matrix form.
- How can we generate all 4×4 involutory and MDS matrix representatives, which will provide us to generate all involutory and MDS matrices for this size?

The answer is to look at the generic properties of a Hadamard matrix satisfying the involutory property as given in the matrix form H: XOR sum of the elements in any row or column of a Hadamard matrix is equal to 1 and XOR sum of the elements in the main diagonal is equal to 0.

How to generate all 4×4 involutory MDS matrices over binary field extensions

- Note that these properties also force XOR sum of the elements in the antidiagonal (counter diagonal) to be equal to 0. In this respect, one can easily define the matrix form R in order to search for all representative involutory MDS matrices over $\mathbb{F}_{2^m}$ as follows:

$$R = \begin{bmatrix} a & d & e & a+d+e+1 \\ f & b & d+e+f+g+h & b+d+e+g+h+1 \\ g & h & c & c+g+h+1 \\ a+f+g+1 & b+d+h+1 & c+d+f+g+h+1 & a+b+c \end{bmatrix}.$$

- The matrix form R above is defined by 8 elements $(a, b, ..., h)$ over $\mathbb{F}_{2^m}$. Then, the search space for finding involutory and MDS matrix representatives is $(2^m - 1)^8$. For example, for $\mathbb{F}_{2^4}$, the search space is $(2^4 - 1)^8 \approx 2^{31.25}$.

How to generate all 4×4 involutory MDS matrices over binary field extensions

- We searched for all possible 4×4 involutory and MDS representatives over $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^4}$. We have found 48 and 71,856 (wheras a 4×4 Hadamard matrix is generating 1512) involutory and MDS representative matrices, respectively.

- As a result, after applying the parameters (b_is) to involutory and MDS representative matrices, we generated totally $48 \cdot (2^3 - 1)^3 = 16,464$ and $71856 \cdot (2^4 - 1)^3 = 242,514,000 \approx 2^{27.85}$ 4×4 involutory and MDS matrices over $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^4}$, respectively.

How to generate all 4×4 involutory MDS matrices over binary field extensions

Example

Let $\mathbb{F}_{2^4}$ be generated by the primitive element α which is a root of the primitive polynomial $x^4 + x + 1$ ($\texttt{0x13}$). Consider the 4×4 θ-circulant involutory MDS matrix recently given in [10]

$$M_2 = \begin{bmatrix} \alpha & 1 & \alpha^{14} & \alpha^7 \\ \alpha^{14} & \alpha^2 & 1 & \alpha^{13} \\ \alpha^{11} & \alpha^{13} & \alpha^4 & 1 \\ 1 & \alpha^7 & \alpha^{11} & \alpha^8 \end{bmatrix}$$

over $\mathbb{F}_{2^4}/\texttt{0x13}$. In fact, the involutory MDS matrix M_2 belongs to a class of which representative involutory MDS matrix is as follows:

How to generate all 4×4 involutory MDS matrices over binary field extensions

Example

$$MR_2 = \begin{bmatrix} \alpha & \alpha^7 & \alpha^5 & \alpha^{11} \\ \alpha^7 & \alpha^2 & \alpha^{14} & \alpha^{10} \\ \alpha^5 & \alpha^{14} & \alpha^4 & \alpha^{13} \\ \alpha^{11} & \alpha^{10} & \alpha^{13} & \alpha^8 \end{bmatrix}$$

which is symmetric and also 4×4 θ-circulant involutory MDS matrix. The matrix M_2 can easily be obtained by applying the parameters $b_1 = \alpha^8$, $b_2 = \alpha^9$ and $b_3 = \alpha^{11}$ to MR_2.

How to generate all 4×4 involutory MDS matrices over binary field extensions

Example

Let $\mathbb{F}_{2^4}$ be generated by the primitive element α which is a root of the primitive polynomial $x^4 + x + 1$ ($\texttt{0x13}$). Consider one of 4×4 involutory and MDS representative matrices given below:

$$MR_3 = \begin{bmatrix} 1 & \alpha^5 & \alpha^3 & \alpha^{11} \\ \alpha^{13} & 1 & \alpha^4 & \alpha^{11} \\ \alpha^{11} & \alpha^{11} & \alpha^{12} & \alpha^{11} \\ \alpha^4 & \alpha^3 & \alpha^8 & \alpha^{12} \end{bmatrix}$$

over $\mathbb{F}_{2^4}/\texttt{0x13}$. Then, one can generate 4×4 involutory and MDS matrix M_3 by applying the parameters $b_1 = 1$, $b_2 = \alpha^{11}$ and $b_3 = \alpha^4$ to MR_3 with the least naive XOR count 75 among the ones having the maximum number of occurences of 1s.

How to generate all 4×4 involutory MDS matrices over binary field extensions

Example

$$M_3 = \begin{bmatrix} 1 & \alpha^5 & \alpha^{14} & 1 \\ \alpha^{13} & 1 & 1 & 1 \\ 1 & 1 & \alpha^{12} & \alpha^4 \\ 1 & \alpha^{14} & 1 & \alpha^{12} \end{bmatrix}.$$

This matrix can be implemented by 47 XORs after using optimization technique SLP.

Note that in this presentation for the first time the maximum number of occurrences of 1s for 4×4 involutory and MDS matrices is shown to be 9.

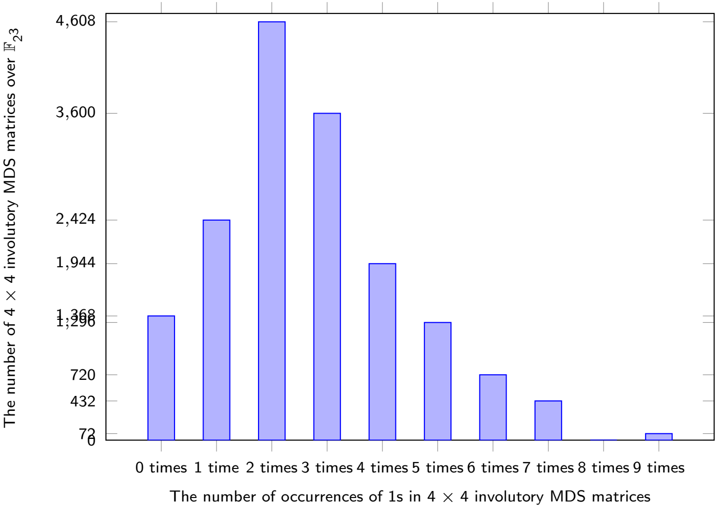
In the next slide, the distribution of the number of occurrences of 1s in all 4×4 involutory MDS matrices over $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^4}$ is presented.

How to generate all 4×4 involutory MDS matrices over binary field extensions

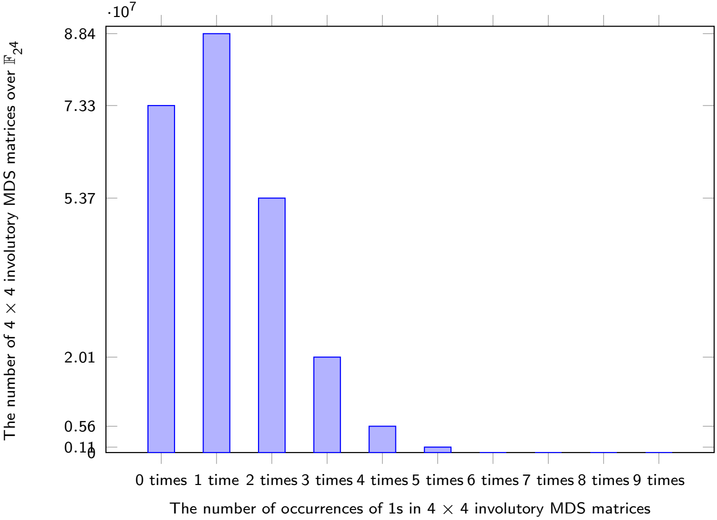
	The number of occurrences of 1s in 4×4 involutory MDS matrices									
Time/Times	0	1	2	3	4	5	6	7	8	9
The number of 4×4 involutory MDS matrices over $\mathbb{F}_{2^3}$	1,368	2,424	4,608	3,600	1,944	1,296	720	432	0	72

	The number of occurrences of 1s in 4×4 involutory MDS matrices									
Time/Times	0	1	2	3	4	5	6	7	8	9
The number of 4×4 involutory MDS matrices over $\mathbb{F}_{2^4}$	73,266,816	88,442,736	53,722,608	20,148,576	5,555,760	1,146,768	206,160	21,120	3,264	192

How to generate all 4×4 involutory MDS matrices over binary field extensions



How to generate all 4×4 involutory MDS matrices over binary field extensions



Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

- This section is on how to obtain the isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$.
- A novel method is given to obtain distinct functions related to these automorphisms and isomorphisms to be used in generating isomorphic MDS matrices (new MDS matrices in view of implementation properties) using the existing ones.

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Proposition

Let A be a $k \times k$ matrix over the finite field $\mathbb{F}_{2^m}$. Let A' be generated by applying any distinct automorphism $f_i : b \mapsto b^{2^i}$ to the elements of A with $0 \leq i \leq m-1$ and $b \in \mathbb{F}^*_{2^m}$. Then, the determinant of A' is equal to 0 if and only if the determinant of A is equal to 0.

Proof.

By Theorem 2.21 in [11], the automorphisms of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ are given as b^{2^i} for all nonzero $b \in \mathbb{F}_{2^m}$ and $0 \leq i \leq m-1$. These mappings are one-to-one because each element in $\mathbb{F}_2$ maps to itself. Since the mappings are distinct, the determinant is related to the automorphism. Then, the determinant of any matrix generated by applying any distinct automorphism to A remains unchanged being either zero or nonzero, i.e., if $\det(A) \neq 0$ or $\det(A) = 0$, then $det(A') \neq 0$ or $\det(A') = 0$, respectively. □

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Theorem

There exist $m \cdot (2^m - 1)$ distinct and bijective functions related to the automorphisms in the form of $f_{i,c} : \beta \mapsto (\beta^{2^i}) \cdot c$, where β is any primitive element of $\mathbb{F}_{2^m}$, $c \in \mathbb{F}_{2^m}^*$ and $0 \leq i \leq m - 1$. These functions preserve the MDS property of a square matrix over the same binary field extension, i.e., new MDS matrices are generated from the existing ones.

Proof.

Here we need to show that the properties of being an MDS matrix are satisfied after applying distinct functions.The main idea depends on the fact that every square submatrix of an MDS matrix is nonsingular. We divide the proof into three parts. Note that all elements of an MDS matrix must be nonzero. Let $p(x)$ be an irreducible polynomial of degree m over $\mathbb{F}_2$ and $\beta \in \mathbb{F}_{2^m}$ be a primitive element. We divide the proof into three parts.

□

Proof.

- Let $f_i : x \mapsto x^{2^i}$, then we have $\det A' = f_i(\det A)$. If $\det A \neq 0$, then $f_i(\det A) \neq 0$ since f_i is an automorphism.
- Let $g_c(x) \mapsto c \cdot x$, where $c \in \mathbb{F}_{2^m}^*$, then $\det A' = c \cdot \det A$ from elementary linear algebra. Since $c \neq 0$ and $\det A \neq 0$, $\det A' \neq 0$.
- Now, let $f_{i,c} = g_c(\beta) \circ f_i(\beta) = g_c(f_i(\beta)) = c \cdot \beta^{2^i}$. Then, $\det A' = c \cdot f_i(\det A)$. Since $\det A \neq 0$, $\det A' \neq 0$.

Note that if $\det A' \neq 0$, then we obtain $\det A \neq 0$ by considering $\det A = f_{m-i}(\frac{1}{c} \det A')$. Since every square submatrix of A is invertible and each row or column of A is linearly independent, the MDS property is preserved. In conclusion, $\det A' \neq 0$ if and only if $\det A \neq 0$. $\square$

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Example

Let $\mathbb{F}_{2^4}$ be defined by the primitive polynomial $p(x) = x^4 + x + 1$. Let α be a root of $p(x)$. Then, $M_1 = had(1_h, 2_h, 4_h, 6_h) = had(1, \alpha, \alpha^2, \alpha^5)$ is an involutory 4×4 MDS matrix.

By the given Theorem, consider $f_{2,1} : \alpha \mapsto \alpha^4$ automorphism. Then, the new involutory 4×4 MDS matrix generated from M_4 by $f_{2,1}$ is as follows: $M_4' = had(1_h, 3_h, 5_h, 6_h) = had(1, \alpha^4, \alpha^8, \alpha^5)$.

M_4' is called an automorphism of M_4 under $f_{2,1} : \alpha \mapsto \alpha^4$. Note that by the given Theorem, one can generate 59 more MDS matrices by using the MDS matrix M_4.

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Proposition

Let A be a $k \times k$ matrix over the finite field $\mathbb{F}_{2^m}/p_1(x)$ and β_1 be any primitive element of $\mathbb{F}_{2^m}/p_1(x)$. Let A' be a $k \times k$ matrix over the finite field $\mathbb{F}_{2^m}/p_2(x)$ generated by applying the isomorphism $f_{s_u} : \beta_1 \mapsto \beta_2^{s_u}$ to the elements of A (which can also be represented as β_1^d for $0 \leq d \leq 2^m - 2$), where β_2 is any primitive element of $\mathbb{F}_{2^m}/p_2(x)$, $s_u = e \cdot 2^i$ for $1 \leq e \leq 2^m - 2$, $gcd(e, 2^m - 1) = 1$, $p_1(\beta_2^{s_u}) = 0$ and $0 \leq u, i \leq m - 1$. Then, the determinant of A' is equal to 0 if and only if the determinant of A is equal to 0.

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Proof.

The proof is similar to Proposition given for automorphisms since we have the same mapping up to the isomorphism and all entries of an MDS matrix remain nonzero after applying the isomorphism. Note that each f_{s_u} maps each element in $\mathbb{F}_2$ to itself. The isomorphism f_{s_u} is related to automorphism defined in Proposition given for automorphisms due to the structure of s_u. □

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Theorem

There exist $m \cdot (2^m - 1)$ distinct functions obtained by using isomorphisms in the form of $f_{s_u,c} : \beta_1 \mapsto (\beta_2^{s_u}) \cdot c$, where β_1 and β_2 are respectively any primitive element of $\mathbb{F}_{2^m}/p_1(x)$ and $\mathbb{F}_{2^m}/p_2(x)$, $c \in \mathbb{F}_{2^m}^*$, $s_u = e \cdot 2^i$ for $1 \leq e \leq 2^m - 2$, $gcd(e, 2^m - 1) = 1$, $p_1(\beta_2^{s_u}) = 0$ and $0 \leq u, i \leq m - 1$. These functions can be used in generating new MDS matrices over $\mathbb{F}_{2^m}/p_2(x)$ from an MDS matrix over $\mathbb{F}_{2^m}/p_1(x)$, which preserve the MDS property of a square matrix.

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Proof.

Let $\beta \in \mathbb{F}_{2^m}$ be a primitive element. Recall that the minimal polynomial of the set $\beta, \beta^2, \ldots, \beta^{2^{m-1}}$, where m is the smallest integer such that $\beta^{2^m} = \beta$, is the same. Since the proof is similar to Theorem for automorphisms, we omit it. □

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Algorithm 1 Computing s_u values to define the isomorphisms in given Proposition

```
1: for s_u = 1 to 2^m − 2 do
2:     y_1 ← p_1(β_2^{s_u}) (mod p_2(x))
3:     if y_1 = 0 then
4:         Return (s_u)
5:     end if
6: end for
```

INPUT: $p_1(\beta_1)$, β_2 and $p_2(x)$
OUTPUT: $s_u = e \cdot 2^i$ with $gcd(e, 2^m - 1) = 1$, where $0 \leq u, i \leq m - 1$

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Example

Let $\mathbb{F}_{2^4}$ be defined by the irreducible polynomial $p_1(x) = x^4 + x^3 + x^2 + x + 1$. Then, β_1 defined by $\beta_1 = \alpha + 1$ is a primitive element, where α is a root of $p_1(x)$.

$M_5 = had(1_h, 2_h, 4_h, 6_h) = had(1, \beta_1^{12}, \beta_1^{9}, \beta_1^{13})$ is an involutory 4×4 MDS matrix over $\mathbb{F}_{2^4}/p_1(x)$.

We can rewrite $p_1(\alpha) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$ in terms of β_1 as $p_1(\beta_1) = \beta_1^4 + \beta_1^3 + 1$.

Consider the finite field $\mathbb{F}_{2^4}/p_2(x)$, where $p_2(x) = x^4 + x + 1$. Let the primitive element β_2 of $\mathbb{F}_{2^4}/p_2(x)$ be α_1, which is also a root of $p_2(x)$.

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Example

Then, we can obtain 4 distinct isomorphisms from $\mathbb{F}_{2^4}/p_1(x)$ to $\mathbb{F}_{2^4}/p_2(x)$ by computing s_u values (which are $s_0 = 7$, $s_1 = 11$, $s_2 = 13$ and $s_3 = 14$) in Algorithm 1.

These isomorphisms are $f_{7,1} : \beta_1 \mapsto \alpha_1^7$, $f_{11,1} : \beta_1 \mapsto \alpha_1^{11}$, $f_{13,1} : \beta_1 \mapsto \alpha_1^{13}$ and $f_{14,1} : \beta_1 \mapsto \alpha_1^{14}$.

For example, by using the isomorphism $f_{7,1} : \beta_1 \mapsto \alpha_1^7$, we can generate the involutory 4×4 MDS matrix M_5' over $\mathbb{F}_{2^4}/p_2(x)$ from M_5 over $\mathbb{F}_{2^4}/p_1(x)$ as follows: $M_5' = had(1_h, A_h, 8_h, 2_h) = had(1, \alpha_1^9, \alpha_1^3, \alpha_1)$.

MAGMA code for obtaining s_u values

```
P<z> := PolynomialRing(GF(2));
p := z^4+z+1;
F<x> := ext <GF(2) | p >;

for su:= 1 to 14 do
  y1:=(x^su)^4 + (x^su)^3 + 1;
    if (y1 eq 0) then PrintFile ("power.txt",su);
    end if;
end for;
```

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

A general method to obtain the isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$ (where $t \geq 1$ and $m > 1$) and distinct functions related to these isomorphisms can be given as follows:

1- Choose a primitive polynomial $p_1(x)$ of degree m and the primitive elements β_1 and β_2 for the finite fields $\mathbb{F}_{2^m}/p_1(x)$ and $\mathbb{F}_{2^{mt}}/p_2(x)$, respectively.

2- Generate m isomorphisms, i.e., compute s_u values by using Algorithm 2.

3- Compute $m \cdot (2^{mt} - 1)$ distinct functions related to the isomorphisms by multiplying the isomorphisms generated in Step 2 with all nonzero constants $c \in \mathbb{F}_{2^{mt}}$.

Remark

Let $p_1(x)$ be an irreducible polynomial but not primitive in Step 1. Then, a primitive polynomial is constructed by evaluating β_1 in $p_1(x)$, i.e., $p_1(\beta_1)$. This polynomial is used as an input to Algorithm 2.

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Algorithm 2 Computing s_u values to define the isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$.

1: **for** $s_u = 1$ to $2^{mt} - 2$ **do**
2: $\quad y_1 \leftarrow p_1(\beta_2^{s_u}) \pmod{p_2(x)}$
3: $\quad$ **if** $y_1 = 0$ **then**
4: $\quad\quad$ Return s_u
5: $\quad$ **end if**
6: **end for**

INPUT: $p_1(\beta_1)$, β_2 and $p_2(x)$
OUTPUT: s_u, where $0 \leq u \leq m - 1$

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Example

Let $\mathbb{F}_{2^4}$ be defined by the primitive polynomial $p_1(x) = x^4 + x + 1$. Let α be a root of $p_1(x)$. Then,

$$M_6 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^4 \\ 1 & 1 & \alpha^3 & \alpha^2 \\ 1 & \alpha^2 & 1 & \alpha \\ \alpha & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1_h & 2_h & 4_h & 3_h \\ 1_h & 1_h & 8_h & 4_h \\ 1_h & 4_h & 1_h & 2_h \\ 2_h & 1_h & 1_h & 1_h \end{bmatrix}$$ is an involutory 4×4 MDS matrix over $\mathbb{F}_{2^4}/p_1(x)$.

Consider the finite field $\mathbb{F}_{2^8}/p_2(x)$, where $p_2(x) = x^8 + x^4 + x^3 + x + 1$. Let the primitive element β_2 of $\mathbb{F}_{2^8}/p_2(x)$ be $\alpha_1 + 1$, where α_1 is a root of $p_2(x)$. Then, we can obtain 4 distinct isomorphisms from $\mathbb{F}_{2^4}/p_1(x)$ to $\mathbb{F}_{2^8}/p_2(x)$ by computing s_u values in Algorithm 2.

MAGMA code for obtaining s_u values

```
P<z> := PolynomialRing(GF(2));
p := z^8 + z^4 + z^3 + z+1;
F<x> := ext <GF(2) | p >;

for su:= 1 to 254 do
  y1:=((x+1)^su)^4 + ((x+1)^su)^1 + 1;
    if (y1 eq 0) then PrintFile ("power.txt",su);
    end if;
end for;
```

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

Example

These isomorphisms are $f_{17,1} : \alpha \mapsto \beta_2^{17}$, $f_{34,1} : \alpha \mapsto \beta_2^{34}$, $f_{68,1} : \alpha \mapsto \beta_2^{68}$ and $f_{136,1} : \alpha \mapsto \beta_2^{136}$. For example, by using the isomorphism $f_{17,1} : \alpha \mapsto \beta_2^{17}$, we can generate the involutory 4×4 MDS matrix M_6' over $\mathbb{F}_{2^8}/p_2(x)$ from M_6 over $\mathbb{F}_{2^4}/p_1(x)$ as follows:

$$M_6' = \begin{bmatrix} 1 & \beta_2^{17} & \beta_2^{34} & \beta_2^{68} \\ 1 & 1 & \beta_2^{51} & \beta_2^{34} \\ 1 & \beta_2^{34} & 1 & \beta_2^{17} \\ \beta_2^{17} & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 01_h & E1_h & 5C_h & E0_h \\ 01_h & 01_h & 0C_h & 5C_h \\ 01_h & 5C_h & 01_h & E1_h \\ E1_h & 01_h & 01_h & 01_h \end{bmatrix}.$$

Note that one can generate 1019 $(4 \cdot (2^8 - 1) - 1)$ more MDS matrices over $F_{2^8}/p_2(x)$ by using the MDS matrix M_6 over $\mathbb{F}_{2^4}/p_1(x)$.

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

- The method described takes an MDS matrix as input to generate new MDS matrices. It may help other construction methods to generate isomorphic MDS matrices, which may have better implementation properties than the ones constructed by the other construction methods in the literature. Some important properties of the method can be given as follows:
- The method is intended to be applied to other construction methods in the literature to generate new MDS matrices from the existing ones.
- The method can be considered as a complementary method for the current construction methods allowing them looking for MDS matrices having better implementation properties through mapping them to different field representations.

Isomorphisms between MDS matrices over $\mathbb{F}_{2^m}$ and MDS matrices over $\mathbb{F}_{2^{mt}}$, where $t \geq 1$ and $m > 1$

- The method helps to map any $k \times k$ MDS matrix over $\mathbb{F}_{2^m}$ to its corresponding isomorphic $k \times k$ MDS matrix over $\mathbb{F}_{2^{mt}}$.
- An MDS matrix generated over $\mathbb{F}_{2^{mt}}$ from an existing MDS matrix over $\mathbb{F}_{2^m}$ can take the advantage of small number of table lookups in the implementation, which can only be used with XOR operations. By the help of isomorphisms, it can also be implemented by the same number XOR operations and table lookups with that of an existing MDS matrix over $\mathbb{F}_{2^m}$.
- The method helps to generate MDS matrices over $\mathbb{F}_{2^{mt}}$ with efficient software implementations when mt is large.

Conclusions

- In this presentation, we tried to put a different perspective on the design of (involutory) MDS matrices.
- We looked for the answer to the question of what a Hadamard matrix actually is.
- A Hadamard matrix (is a matrix form) generates some representative matrices that can be used to generate involutory and MDS matrices. For 2×2 involutory MDS matrices, Hadamard matrix form can be used to generate all representatives. For other sizes, e.g. 4×4 involutory MDS matrices, some of the representative matrices can be generated by Hadamard matrix form.

Conclusions

- We presented a new method generating all 4×4 involutory and MDS matrices, which shows that there is a more general form including Hadamard matrix. This method approximately reduces the search space to the level of $\sqrt{n}$, where n represents the number of all 4×4 matrices.
- Finally, we described a new method to be used as a complementary method for the current construction methods allowing them looking for MDS matrices having better implementation properties through mapping them to different field representations.

References I

[1] F. J. MacWilliams, and N. J. A. Sloane: The Theory of Error Correcting Codes, North Holland, 1986.

[2] 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.

[3] J. Lacan, J. Fimes, Systematic MDS erasure codes based on vandermonde matrices, IEEE Trans. Commun. Lett., vol. 8, pp. 570-572, 2004.

[4] 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.

[5] S. Sarkar, H. Syed, Lighweight Diffusion Layer: Importance of Toeplitz Matrices, IACR Transactions on Symmetric Cryptology, vol.2016(1), pp. 95-113, 2016.

[6] Sim, S.M., Khoo, K., Oggier, F., Peyrin, T.: 'Lightweight MDS involution matrices', Fast Software Encryption (FSE 2015), LNCS 9054, pp.471-493.

References II

[7] Khoo, K., Peyrin, T., Poschmann, A.Y., Yap, H.: 'FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison', Cryptographic Hardware and Embedded Systems (CHES 2014), LNCS 8731, pp. 433-450.

[8] M.K. Pehlivanoğlu, M.T. Sakallı, 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.

[9] G.G. Güzel, M.T. Sakallı, S. Akleylek, V. Rijmen, Yasemin Çengellenmiş, A new matrix form to generate all 3×3 involutory MDS matrices over F_{2^m}, Information Processing Letters, vol. 147, pp. 61-68, 2019.

[10] V. Cauchois, P. Loidreau, On circulant involutory MDS matrices, Designs, Codes and Cryptography, vol. 87, pp. 249-260, 2019.

[11] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1986.

[12] M.T. Sakallı, S. Akleylek, Kemal Akkanat, V. Rijmen, On the Automorphisms and Isomorphisms of MDS Matrices and Their Efficient Implementations (submitted)

Thank you for your attention!