On the Construction of Lightweight Circulant Involutory MDS matrices

Yongqiang Li[1,2], Mingsheng Wang[1]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences

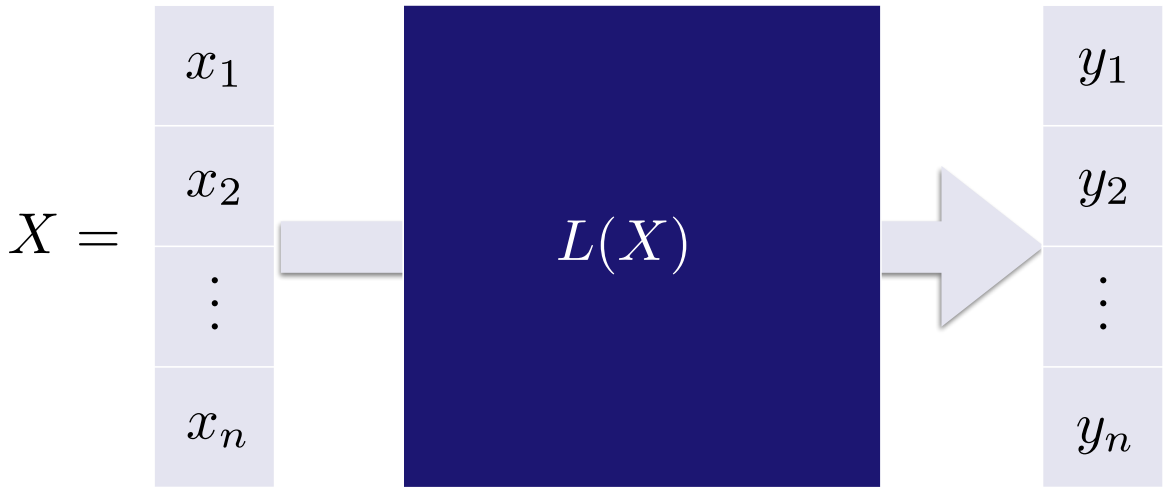
[2] Science and Technology on Communication Security Laboratory

FSE 2016, Bochum, Germany

March 21, 2016

Liner Diffusion Layer

A linear mapping provides internal dependency.



The performance is measured by branch number:

- $\mathcal{B}(L) = \min\{\omega_b(X) + \omega_b(L(X)) \mid X \in (\mathbb{F}_2^m)^n, X \neq 0\}$;
- $\mathcal{B}(L) \leq n + 1$.

Lightweight MDS Matrix

MDS matrix

Let L be a linear mapping over $(\mathbb{F}_2^m)^n$, i.e. L is a linear mapping acts on n S-boxes, and each S-box is of m-bit length. Then L is called an MDS matrix if $\mathcal{B}(L) = n + 1$.

An MDS matrix can be represented by the following matrix:

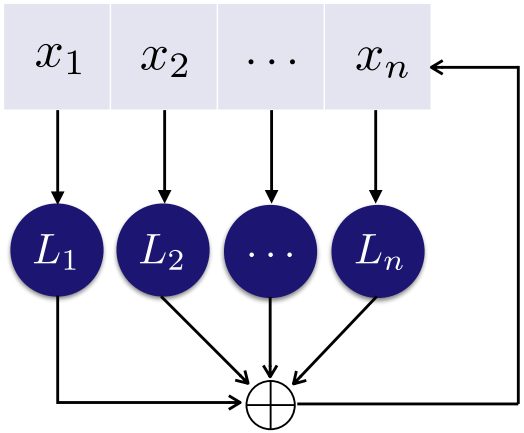
$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix},$$

where $L_{i,j}$ are $m \times m$ matrices over $\mathbb{F}_2$.

Lightweight means the implementation requires fewer XORs.

Previous Construction Methods

- Recursive constructions—Based on LFSRs



  - Light but high latency

- Direct constructions—Based on finite fields
  - Implement the multiplication of entries of finite fields

The entries are always pairwise commutative. Why?

The Advantage of Commutative Entries

It is very efficient to characterize whether L is MDS or not.

Blaum, Roth, IEEE TIT 1999

L is MDS if and only if every square sub-matrices of L are non-singular.

- The determinants of square sub-matrices of L can be computed;
- The determinants can be factorized;
- One can get an equivalent condition set.

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \ldots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix}$$

The Disadvantages of Commutative Entries

- Some interesting MDS matrices are proved do not exist.
  - Nakahara, Abraho, IJNS 2009:
    4×4 circulant involutory MDS matrix does not exist.
  - Gupta, Ray, CCDS 2015:
    $n \times n$ circulant involutory MDS matrix does do not exist.
  - Gupta, Ray, CCDS 2015:
    $2^d \times 2^d$ circulant orthogonal MDS matrix does not exist.

The Disadvantages of Commutative Entries

- Some interesting MDS matrices are proved do not exist.
  - Nakahara, Abraho, IJNS 2009:
    4×4 circulant involutory MDS matrix does not exist over finite fields.
  - Gupta, Ray, CCDS 2015:
    $n \times n$ circulant involutory MDS matrix does do not exist over finite fields.
  - Gupta, Ray, CCDS 2015:
    $2^d \times 2^d$ circulant orthogonal MDS matrix does not exist over finite fields.

The Disadvantages of Commutative Entries

- Some interesting MDS matrices are proved do not exist.
  - Nakahara, Abraho, IJNS 2009:
    4×4 circulant involutory MDS matrix does not exist over finite fields.
  - Gupta, Ray, CCDS 2015:
    $n \times n$ circulant involutory MDS matrix does do not exist over finite fields.
  - Gupta, Ray, CCDS 2015:
    $2^d \times 2^d$ circulant orthogonal MDS matrix does not exist over finite fields.
- May lose MDS matrices with fewer XORs.

Motivations and Methods

Construct MDS matrices with non-commutative entries.

Goals

- Construct some MDS matrices that have been proved do not exist when the entries are commutative.
- Construct MDS matrices with as few XORs as possible.
  - Give lower bounds of XORs of some MDS matrices and corresponding constructions.

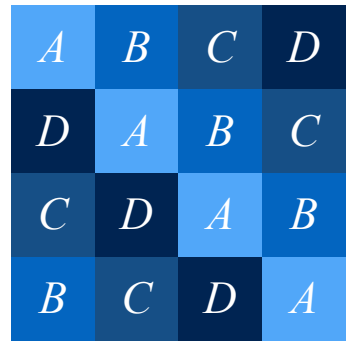
Methods

- Compute the rank of all square sub-matrices to determine whether a matrix is MDS or not.
- Search all possible entries to get lower bounds on XORs.

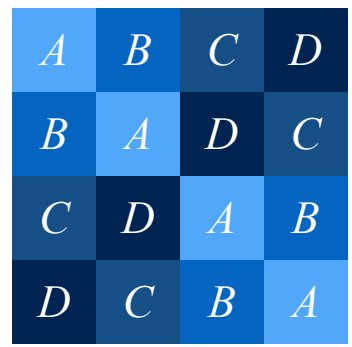
Focus on the Following Special Matrices

$n = 4, m = 4, 8.$

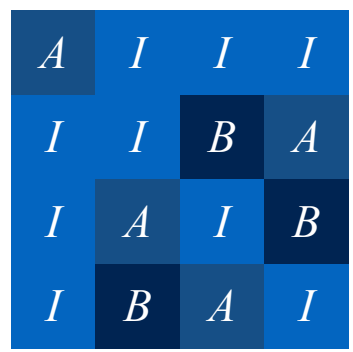
- Circulant MDS matrix.
  - Involutory.
  - Non-involutory.
  - Orthogonal.



- Hadamard MDS matrix.
  - Involutory.
  - Non-involutory.



- "Optimal" 4×4 MDS matrix.



A General Lower Bound on XORs of Entries

The number of entries with no XORs is limited.

A general bound

Let $A, B, C, D \in GL(m, \mathbb{F}_2)$. Then

- If $Circ(A, B, C, D)$ is a *circulant MDS matrix*, then $\#A + \#B + \#C + \#D \geq 2$.
- If $Had(A, B, C, D)$ is a *Hadamard MDS matrix*, then $\#A + \#B + \#C + \#D \geq 3$.

- There are at most 2 entries with no XORs in one row of a circulant MDS matrix;
- There are at most 1 entry with no XORs in one row of a Hadamard MDS matrix.
- We suppose $L[1, 1] = I$ in the following constructions.

Trick for Searching

Using sub-matrices of order 2 to reduce searching space.

Trick for Searching

Using sub-matrices of order 2 to reduce searching space.

$$L = Circ(I, I, A, B) = \begin{pmatrix} I & I & A & B \\ B & I & I & A \\ A & B & I & I \\ I & A & B & I \end{pmatrix}.$$

Trick for Searching

Using sub-matrices of order 2 to reduce searching space.

$$L = Circ(I, I, A, B) = \begin{pmatrix} I & I & A & B \\ B & I & I & A \\ A & B & I & I \\ I & A & B & I \end{pmatrix}.$$

Fact

If $L = Circ(I, I, A, B)$ is MDS, then all its square sub-matrices of order 2 are non-singular.

Trick for Searching

Using sub-matrices of order 2 to reduce searching space.

$$\begin{pmatrix} B & A \\ I & I \end{pmatrix}, \begin{pmatrix} A & B \\ B & I \end{pmatrix}, \begin{pmatrix} B & I \\ A & I \end{pmatrix}, \begin{pmatrix} B & A \\ A & I \end{pmatrix},$$
$$\begin{pmatrix} I & B \\ B & A \end{pmatrix}, \begin{pmatrix} B & I \\ I & B \end{pmatrix}, \begin{pmatrix} B & I \\ A & B \end{pmatrix}, \begin{pmatrix} A & I \\ I & B \end{pmatrix},$$
$$\begin{pmatrix} B & I \\ I & A \end{pmatrix}, \begin{pmatrix} I & A \\ I & I \end{pmatrix}, \begin{pmatrix} I & A \\ A & I \end{pmatrix}, \begin{pmatrix} I & B \\ I & I \end{pmatrix},$$
$$\begin{pmatrix} I & B \\ A & I \end{pmatrix}, \begin{pmatrix} A & I \\ I & A \end{pmatrix}, \begin{pmatrix} I & A \\ I & B \end{pmatrix}, \begin{pmatrix} I & I \\ A & B \end{pmatrix},$$
$$\begin{pmatrix} I & I \\ I & A \end{pmatrix}, \begin{pmatrix} I & A \\ A & B \end{pmatrix}, \begin{pmatrix} A & B \\ I & I \end{pmatrix}, \begin{pmatrix} I & B \\ I & A \end{pmatrix},$$
$$\begin{pmatrix} I & I \\ B & I \end{pmatrix}, \begin{pmatrix} A & B \\ I & A \end{pmatrix}, \begin{pmatrix} I & A \\ B & I \end{pmatrix}, \begin{pmatrix} I & B \\ B & I \end{pmatrix}.$$

Trick for Searching

Using sub-matrices of order 2 to reduce searching space.

Lemma

Let $A, B, C \in GL(m, \mathbb{F}_2)$ are $m \times m$ non-singular matrices over $\mathbb{F}_2$. Then the following statements hold.

1. $\begin{pmatrix} I, & A \\ B, & C \end{pmatrix}$ *is non-singular* $\iff \operatorname{rank}(BA + C) = m.$
2. $\begin{pmatrix} A, & I \\ B, & C \end{pmatrix}$ *is non-singular* $\iff \operatorname{rank}(CA + B) = m.$
3. $\begin{pmatrix} A, & B \\ I, & C \end{pmatrix}$ *is non-singular* $\iff \operatorname{rank}(AC + B) = m.$
4. $\begin{pmatrix} A, & B \\ C, & I \end{pmatrix}$ *is non-singular* $\iff \operatorname{rank}(BC + A) = m.$

Trick for Searching

Using sub-matrices of order 2 to reduce searching space.

Conditions

If $L = Circ(I, I, A, B)$ is MDS, then the following matrix are non-singular:

$$A + I, B + I, A + B, AB + I, A^2 + B, A + B^2.$$

Trick for Searching

Using sub-matrices of order 2 to reduce searching space.

Conditions

If $L = Circ(I, I, A, B)$ is MDS, then the following matrix are non-singular:

$$A + I, B + I, A + B, AB + I, A^2 + B, A + B^2.$$

Trick for Searching

Using sub-matrices of order 2 to reduce searching space.

Conditions

If $L = Circ(I, I, A, B)$ is MDS, then the following matrix are non-singular:

$$A + I, B + I, A + B, AB + I, A^2 + B, A + B^2.$$

$A, B \in S_{A,B} := \{X \mid \text{rank}(X + I) = m\}$.

Trick for Searching

Using sub-matrices of order 2 to reduce searching space.

Conditions

If $L = Circ(I, I, A, B)$ is MDS, then the following matrix are non-singular:

$$A + I, B + I, A + B, AB + I, A^2 + B, A + B^2.$$

$A, B \in S_{A,B} := \{X \mid \text{rank}(X + I) = m\}$.

Searching method

---

for $A \in S_{A,B}$

$S_B := \{B \in S_{A,B} \mid \text{rank}(A + B) = \text{rank}(AB + I)$
$= \text{rank}(A^2 + B) = \text{rank}(A + B^2) = m\}$

for $B \in S_B$

test whether $Circ(I, I, A, B)$ is MDS

Lightweight Circulant Non-involutory MDS Matrix

Searching: Magma v2.20-3, Laptop (OSX 10.9, Intel Core i7);

It takes nearly *3 days* to get the following result:

Theorem

Let $L = Circ(I, I, A, B)$, *where* $A, B \in GL(m, \mathbb{F}_2)$, $m = 4, 8$. *If* L *is an MDS matrix, then* $\#A + \#B \geq 3$. $(48, 80640)$

Lightweight Circulant Non-involutory MDS Matrix

Searching: Magma v2.20-3, Laptop (OSX 10.9, Intel Core i7);

It takes nearly *3 days* to get the following result:

Theorem

Let $L = Circ(I, I, A, B)$, *where* $A, B \in GL(m, \mathbb{F}_2)$, $m = 4, 8$. *If* L *is an MDS matrix, then* $\#A + \#B \geq 3$. $(48, 80640)$

$(48, 80640)$ means there are at least 48 and 80640 pairs of $A, B \in GL(m, \mathbb{F}_2)$ such that $Circ(I, I, A, B)$ is MDS and the lower bound on XORs holds for $m = 4$ and $m = 8$ respectively.

Equivalent conditions of circulant involutory matrix

Let $L = Circ(I, A, B, C)$, where $A, B, C \in GL(m, \mathbb{F}_2)$. Then L is an involution if and only if:

$$AB = BA, BC = CB, A^2 = C^2, AC + CA = B^2.$$

Equivalent conditions of circulant involutory matrix

Let $L = Circ(I, A, B, C)$, where $A, B, C \in GL(m, \mathbb{F}_2)$. Then L is an involution if and only if:

$$AB = BA, BC = CB, A^2 = C^2, AC + CA = B^2.$$

A general construction

- $A, C \in GL(m, \mathbb{F}_2)$ with $A^2 = C^2 = I$
- The multiplication order of $A + C$ equals $4k - 2$,where $k > 1$. This means $(A + C)^{4k-2} = I$.
- Let $B = (A + C)^{2k}$

Then the matrix $Circ(I, A, B, C)$ is an involution.

Lightweight Circulant Involutory MDS Matrices

Searching: Magma v2.20-3, Laptop (OSX 10.9, Intel Core i7);

It takes nearly *one week* to get the following result:

Theorem

Their exist circulant involutory MDS matrix over $GL(m, \mathbb{F}_2)$, $m = 4, 8$. *Furthermore, the following statements hold.*

1. $m = 4$, *circulant involutory MDS matrix* $Circ(I, A, B, C)$ *satisfies* $\#A + \#B + \#C \geq 5$. (48)
2. $m = 8$, *if* $\#A \leq 3$ *and* $\#C \leq 3$, *then circulant involutory MDS matrix* $Circ(I, A, B, C)$ *constructed with the above method satisfies* $\#A + \#B + \#C \geq 9$. (40320)
3. $m = 4, 8$, *circulant involutory MDS matrix* $Circ(I, A, B, B, A)$ *satisfies* $\#A + \#B \geq \frac{m}{2}$. $(24, 20160)$

Lightweight Circulant Involutory MDS Matrices

Searching: Magma v2.20-3, Laptop (OSX 10.9, Intel Core i7);

It takes nearly *one week* to get the following result:

Theorem

Their exist circulant involutory MDS matrix over $GL(m, \mathbb{F}_2)$, $m = 4, 8$. *Furthermore, the following statements hold.*

1. $m = 4$, *circulant involutory MDS matrix* $Circ(I, A, B, C)$ *satisfies* $\#A + \#B + \#C \geq 5$. (48)
2. $m = 8$, *if* $\#A \leq 3$ *and* $\#C \leq 3$, *then circulant involutory MDS matrix* $Circ(I, A, B, C)$ *constructed with the above method satisfies* $\#A + \#B + \#C \geq 9$. (40320)
3. $m = 4, 8$, *circulant involutory MDS matrix* $Circ(I, A, B, B, A)$ *satisfies* $\#A + \#B \geq \frac{m}{2}$. $(24, 20160)$

- Circulant orthogonal MDS matrix exists over $GL(m, \mathbb{F}_2)$.

Equivalent conditions of Hadamard involutory matrix

Let $A, B, C \in GL(m, \mathbb{F}_2)$. Then $L = Had(I, A, B, C)$ is an involution if and only if A, B, C are pairwise commutative and $A^2 + B^2 = C^2$.

Lightweight Hadamard Involutory MDS Matrices

Equivalent conditions of Hadamard involutory matrix

Let $A, B, C \in GL(m, \mathbb{F}_2)$. Then $L = Had(I, A, B, C)$ is an involution if and only if A, B, C are pairwise commutative and $A^2 + B^2 = C^2$.

Searching: Magma v2.20-3, Laptop (OSX 10.9, Intel Core i7);
It takes about *one day* to get the following result:

Theorem

1. *Let* $A, B, C \in GL(4, \mathbb{F}_2)$. *If* $L = Had(I, A, B, C)$ *is an MDS involution matrix, then* $\#A + \#B + \#C \geq 6$. (144)
2. *Let* $A \in GL(8, \mathbb{F}_2)$ *with* $\#A \leq 3$. *If* $L = Had(I, A, A^{-1}, A + A^{-1})$ *is an MDS involution matrix, then* $\#A + \#A^{-1} + \#(A + A^{-1}) \geq 10$. (80640)

Lightweight Hadamard Non-involutoty MDS matrices

Searching: Magma v2.20-3, PC (Win7, Intel Core i5);

It takes nearly *4 weeks* to get the following result:

Theorem

1. *Let* $A, B, C \in GL(4, \mathbb{F}_2)$. *If* $L = Had(I, A, B, C)$ *is an MDS matrix, then* $\#A + \#B + \#C \geq 4$. (72)
2. *Let* $A, B \in GL(8, \mathbb{F}_2)$. *If* $L = Had(I, A, A^T, B)$ *is an MDS matrix, then* $\#A + \#A^T + \#B \geq 5$. (622)

Lightweight "Optimal" 4×4 MDS Matrix

$$L = \begin{pmatrix} A & I & I & I \\ I & I & B & A \\ I & A & I & B \\ I & B & A & I \end{pmatrix}$$

Theorem

Let L be a matrix constructed as above, where $A, B \in GL(m, \mathbb{F}_2), m = 4, 8$. If L is an MDS matrix, then

$$4\#A + 3\#B \geq \begin{cases} 13, & m = 4; \text{ (24)} \\ 10, & m = 8. \text{ (40320)} \end{cases}$$

Comparisons with Previous Constructions

Comparisons of non-inonvolutory MDS matrices

Matrix	Entries	The first row	XOR count	Ref.
Circulant	$GL(8, \mathbb{F}_2)$	(I, I, A, B)	**3**+3×8=27	Our paper
Circulant	$\mathbb{F}_{2^8}$/0x11b	(0x02, 0x03, 0x01, 0x01)	14+3×8=38	AES
Hadamard	$GL(8, \mathbb{F}_2)$	(I, A, A^T, B)	**5**+3×8=29	Our paper
Hadamard	$\mathbb{F}_{2^8}$/0x1c3	(0x01, 0x02, 0x04, 0x91)	13+3×8=37	Sim et al.
Subfield-Hadamard	$\mathbb{F}_{2^4}$/0x13	(0x1, 0x2, 0x8, 0x9)	2×(5+3×4)=34	Sim et al.

Comparisons with Previous Constructions

Comparisons of inonvolutory MDS matrices

Matrix	Entries	The first row	XOR count	Ref.
Circulant	$GL(8, \mathbb{F}_2)$	(I, I, A, B)	**9**+3×8=33	Our paper
Hadamard	$GL(8, \mathbb{F}_2)$	$(I, A, A^{-1}, A + A^{-1})$	**10**+3×8=34	Our paper
Subfield-Hadamard	$\mathbb{F}_{2^4}$/0x13	(0x1, 0x4, 0x9, 0xd)	2×(6+3×4)=36	Sim et al.
Hadamard	$\mathbb{F}_{2^8}$/0x165	(0x01, 0x02, 0xb0, 0xb2)	16+3×8=37	Sim et al.
Hadamard	$\mathbb{F}_{2^8}$/0x11d	(0x01, 0x02, 0x04, 0x06)	22+3×8=46	Anubis
Compact Cauchy	$\mathbb{F}_{2^8}$/0x11b	(0x01, 0x12, 0x04, 0x16)	54+3×8=78	Cui et al.
Hadamard-Cauchy	$\mathbb{F}_{2^8}$/0x11b	(0x01, 0x02, 0xfc, 0xfe)	74+3×8=98	Gupta et al.

Comparisons with Previous Constructions

Comparisons of MDS matrices over $\mathbb{F}_2^4$ and $\mathbb{F}_{2^4}$

Matrix	Entries	The first row	XOR count	Ref.
Circulant	$GL(4, \mathbb{F}_2)$	(I, A, B, C)	**3**+3×4=15	Our paper
Involutory circulant	$GL(4, \mathbb{F}_2)$	(I, A, B, C)	**5**+3×4=17	Our paper
Hadamard	$GL(4, \mathbb{F}_2)$	(I, A, B, C)	**4**+3×4=16	Our paper
Hadamard	$\mathbb{F}_{2^4}$/0x13	(0x1, 0x2, 0x8, 0x9)	5+3×4=17	Sim et al.
Involutory Hadamard	$GL(4, \mathbb{F}_2)$	$(I, A, A^{-1}, A + A^{-1})$	**6**+3×4=18	Our paper
Involutory Hadamard	$\mathbb{F}_{2^4}$/0x13	(0x1, 0x4, 0x9, 0xd)	6+3×4=18	Joltik
Involutory Hadamard	$\mathbb{F}_{2^4}$/0x19	(0x1, 0x2, 0x6, 0x4)	6+3×4=18	Prøst

Summary

Construct circulant involutory MDS matrices firstly.

Summary

Construct circulant involutory MDS matrices firstly.

MDS Matrix	m	lower bounds
Involutory $Circ(I, A, B, C)$	$4, 8$	$\#A + \#B + \#C \geq m + 1$
Involutory $Circ(I, A, B, B, A)$	$4, 8$	$\#A + \#B \geq m/2$
Involutory $Had(I, A, B, C)$	$4, 8$	$\#A + \#B + \#C \geq m + 2$
Non-involutory $Circ(I, I, A, B)$	$4, 8$	$\#A + \#B \geq 3$
Non-involutory $had(I, A, B, C)$	4	$\#A + \#B + \#C \geq 4$
Non-involutory $had(I, A, A^T, B)$	8	$\#A + \#A^T + \#C \geq 5$
Orthogonal $Circ(I, A, B, C)$	4	$\#A + \#B + \#C \geq 8$
"optimal" 4×4 MDS matrix	4	$4\#A + 3\#B \geq 13$
"optimal" 4×4 MDS matrix	8	$4\#A + 3\#B \geq 10$

The lower bounds on XORs of "red" MDS matrices can not be improved.

Is the bound of circulant and Hadamard MDS matrices can be improved if we remove the supposition $L[1,1] = I$?

Is the bound of circulant and Hadamard MDS matrices can be improved if we remove the supposition $L[1,1] = I$?

The answer for MDS matrix over $GL(4, \mathbb{F}_2)$ is NO.

Lower bounds on MDS matrix over $GL(4, \mathbb{F}_2)$

Searching: Magma v2.20-3, PC (Win7, Intel Core i5).

After about *50 days* searching, we get the following result.

Theorem

Let $A_1, A_2, A_3, A_4 \in GL(4, \mathbb{F}_2)$, *and* $\mathcal{B} = \sum_{i=1}^{4} \#A_i$.

1. *If* $Circ(A_1, A_2, A_3, A_4)$ *is an MDS matrix, then* $\mathcal{B} \geq 3$;
2. *If* $Circ(A_1, A_2, A_3, A_4)$ *is an involutory MDS matrix, then* $\mathcal{B} \geq 5$;
3. *If* $Had(A_1, A_2, A_3, A_4)$ *is an MDS matrix, then* $\mathcal{B} \geq 4$;
4. *If* $Had(A_1, A_2, A_3, A_4)$ *is an involutory MDS matrix, then* $\mathcal{B} \geq 6$;

Future Problems

1. Construct bigger order, such as 8×8, lightweight MDS matrices with non-commutative entries.
2. Characterize the existence of 8×8 circulant MDS matrix over $GL(4, \mathbb{F}_2)$.
    - *It has been verified that* 8×8 *circulant MDS matrix do not exist over* $\mathbb{F}_{2^4}$ [Khoo et al. CHES 2014].

Thank you!