MDS Matrices with Lightweight Circuits

Sébastien Duval Gaëtan Leurent

Sebastien.Duval@inria.fr

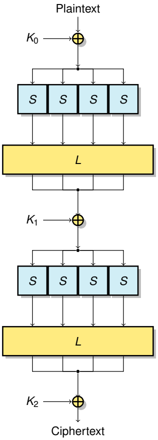
February 14, 2019

Security of Block Ciphers

Shannon's criteria

1. Diffusion
   - Every bit of plaintext and key must affect every bit of the output
   - We usually use linear functions
2. Confusion
   - Relation between plaintext and ciphertext must be intractable
   - Requires non-linear operations
   - Often implemented with tables: S-Boxes

SPN Ciphers



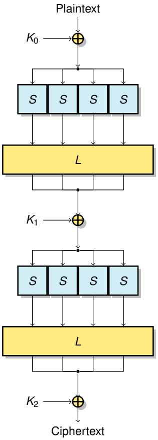
Differential Branch Number

$$\mathcal{B}_d(L) = \min_{x \neq 0}\{w(x) + w(L(x))\}$$

Linear Branch Number

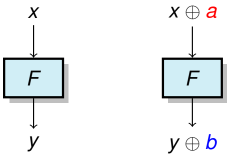
$$\mathcal{B}_l(L) = \min_{x \neq 0}\{w(x) + w(L^\top(x))\}$$

SPN Ciphers

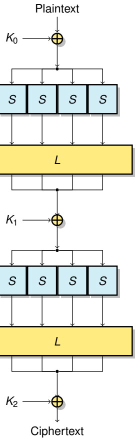


Differential Branch Number

$$\mathcal{B}_d(L) = \min_{x \neq 0}\{w(x) + w(L(x))\}$$



SPN Ciphers



Differential Branch Number

$$\mathcal{B}_d(L) = \min_{x \neq 0}\{w(x) + w(L(x))\}$$

Linear Branch Number

$$\mathcal{B}_l(L) = \min_{x \neq 0}\{w(x) + w(L^\top(x))\}$$

Maximum branch number : $k + 1$
Can be obtained from MDS codes

Diffusion Matrices

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Usually on finite fields:
x a primitive element of $\mathbb{F}_{2^n}$
$2 \leftrightarrow x$
$3 \leftrightarrow x + 1$
Coeffs. $=$ polynomials in x with binary coefficients
i.e. coeffs. $\in \mathbb{F}_2[x]/P$, with P a primitive polynomial

Characterization

L is MDS iff its minors are non-zero

Going Lightweight

lightweight cipher = lightweight S-Boxes + lightweight diffusion matrix

Focus on the diffusion function

Goal: Find lightweight MDS matrix

Main approaches:

- Optimize existing ciphers: MDS matrix → reduce cost (AES MixColumns)
- New ciphers: lightweight by design

Previous Works

Recursive Matrices

Guo, Peyrin and Poschmann in PHOTON (used in LED)
A lightweight matrix
A^i MDS
Implement A, then iterate A i times.

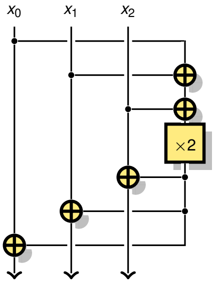
Optimizing Coefficients

- Structured matrices: restrict to a small subspace with many MDS matrices
- More general than finite fields: less costly operations than multiplication in a finite field

Cost Evaluation

Previous work: Number of XORS + sum of cost of each coefficient
Drawback: Cannot reuse intermediate values
Our approach: Global optimization as a circuit

$$\begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{bmatrix}$$

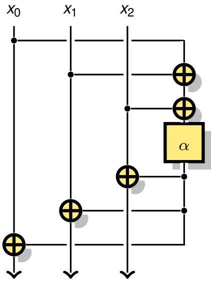


$$\text{Previous: } \begin{cases} 6 \text{ mult. by } 2 \\ 3 \text{ mult. by } 3 \\ 6 \text{ XORS} \end{cases} \qquad \text{New: } \begin{cases} 1 \text{ mult. by } 2 \\ 5 \text{ XORS} \end{cases}$$

Formal Matrices

Finite fields → polynomial ring

- α linear mapping on $\mathbb{F}_{2^n}$
- Coefficients $\in \mathbb{F}_2[\alpha]$
  i.e. polynomials in α with coeffs. in $\mathbb{F}_2$



Formal Matrices

Finite fields → polynomial ring

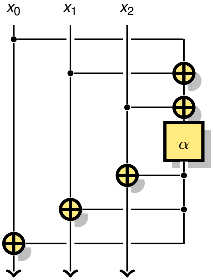
- α linear mapping on $\mathbb{F}_{2^n}$
- Coefficients $\in \mathbb{F}_2[\alpha]$
  i.e. polynomials in α with coeffs. in $\mathbb{F}_2$

Formal matrices

- α undefined

⇒ formal coefficients/matrix

- Objective: find $M(\alpha)$ *s.t.* $\exists A$, $M(A)$ MDS



MDS Characterization of Formal Matrices

MDS Characterization

Maximal branch number iff the minors are non-zero (call it *formal MDS*)
<u>Caution:</u> minors are polynomials in α
$M(\alpha)$ *formal MDS* $\Leftrightarrow \exists A,\ M(A)$ MDS

Objective

- Find $M(\alpha)$ formal MDS and lightweight
- Fix n
- Find A linear mapping over $\mathbb{F}_{2^n}$ lightweight *s.t.* $M(A)$ MDS

Algorithm

Exhaustive search over circuits

Search Space

MDS matrices of sizes 3 × 3 and 4 × 4

For **any** word size *n*

Operations:

- word-wise XOR
- α (generalization of a multiplication)
- Copy

r registers: one register per word (3 for 3 × 3)
+ (at least) one more register → more complex operations

Very costly

Implementation: Main Idea

Graph-based search

- Node = matrix = sequence of operations
- Lightest implementation = shortest path to MDS matrix
- When we spawn a node, we test if it is MDS

Representation

$k \times r$ matrix, coefficients are polynomials in $\mathbb{F}_2[\alpha]$

Optimizations: Cut Useless Branches

Limit use of Copy

After copy, force use of the copied value

Optimizations: Cut Useless Branches

Limit use of Copy

After copy, force use of the copied value

Set up Boundaries

Choose maximum cost and maximum depth for circuits

+ many more optimizations to save memory (at the cost of computation time)

Optimizations: A^*

A^*

Idea of A^*

- Guided Dijkstra
- weight = weight from origin + estimated weight to objective

Optimizations: A^*

A^*

Idea of A^*

- Guided Dijkstra
- weight = weight from origin + estimated weight to objective

Our estimate:

Optimizations: A^*

A^*

Idea of A^*

- Guided Dijkstra
- weight = weight from origin + estimated weight to objective

Our estimate:

- Heuristic
- How far from MDS ?

Optimizations: A^*

A^*

Idea of A^*

- Guided Dijkstra
- weight = weight from origin + estimated weight to objective

Our estimate:

- Heuristic
- How far from MDS ?
- Column with a 0: cannot be part of MDS matrix

Optimizations: A^*

A^*

Idea of A^*

- Guided Dijkstra
- weight = weight from origin + estimated weight to objective

Our estimate:

- Heuristic
- How far from MDS ?
- Column with a 0: cannot be part of MDS matrix
- Linearly dependent columns: not part of MDS matrix

Optimizations: A^*

A^*

Idea of A^*

- Guided Dijkstra
- weight = weight from origin + estimated weight to objective

Our estimate:

- Heuristic
- How far from MDS ?
- Column with a 0: cannot be part of MDS matrix
- Linearly dependent columns: not part of MDS matrix
- Estimate: $m =$ rank of the matrix (without columns containing 0)
- Need at least $k - m$ word-wise XORs to MDS

Result: much faster

Optimizations: Use Equivalence

- `TestedNodes`: list of all nodes that have been tested for MDS
- `UntestedNodes`: list of all untested nodes

Optimizations: Use Equivalence

- `TestedNodes`: list of all nodes that have been tested for MDS
- `UntestedNodes`: list of all untested nodes

Next node = minimal weight/depth node

Optimizations: Use Equivalence

- `TestedNodes`: list of all nodes that have been tested for MDS
- `UntestedNodes`: list of all untested nodes

Next node = minimal weight/depth node
When we test a node M:

Optimizations: Use Equivalence

- `TestedNodes`: list of all nodes that have been tested for MDS
- `UntestedNodes`: list of all untested nodes

Next node = minimal weight/depth node
When we test a node *M*:

- $M \in$`TestedNodes` $\rightarrow$ skip

Optimizations: Use Equivalence

- `TestedNodes`: list of all nodes that have been tested for MDS
- `UntestedNodes`: list of all untested nodes

Next node = minimal weight/depth node
When we test a node M:

- $M \in$`TestedNodes` → skip
- MDS? true → END
- MDS? false → spawn all children nodes in `UntestedNodes`

Optimizations: Use Equivalence

- `TestedNodes`: list of all nodes that have been tested for MDS
- `UntestedNodes`: list of all untested nodes

Next node = minimal weight/depth node
When we test a node M:

- $M \in$`TestedNodes` → skip
- MDS? true → END
- MDS? false → spawn all children nodes in `UntestedNodes`
- Add M to `TestedNodes`

Optimizations: Use Equivalence

- `TestedNodes`: list of all nodes that have been tested for MDS
- `UntestedNodes`: list of all untested nodes

Next node = minimal weight/depth node
When we test a node M:

- $M \in$`TestedNodes` → skip
- MDS? true → END
- MDS? false → spawn all children nodes in `UntestedNodes`
- Add M to `TestedNodes`

Use Equivalence

Matrices are equivalent up to reordering of input/output words
Use unique `ID` for equivalent nodes
Store `TestedIDs` rather than `TestedNodes`

Extensions

Additional Read-only Registers

Allow for use of the input values of the function at any time

Inverse

Allow use of α^{-1}

Powers

Allow use of α^2

Independent Operations

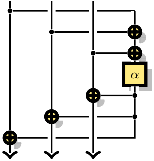
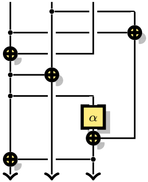
Allow use of 3 independent linear operations α, β, γ

3 × 3 MDS Search

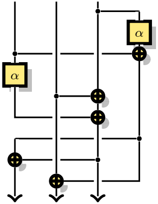
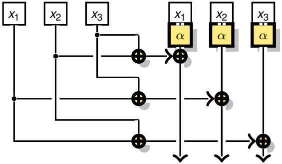
Depth	Cost	Extensions	Memory
4	5 XOR, 1 LIN		14
3	5 XOR, 2 LIN		5
2	6 XOR, 3 LIN	`RO_IN`	4

Table: Optimal 3 × 3 MDS matrices (all results are obtained in less than 1 second, memory is given in MB).

3 × 3 MDS Matrices

Depth	Cost	M	Fig.
4	5 XOR, 1 LIN	$M_{3,4}^{5,1} = \begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{bmatrix}$	
		$M_{3,4}^{5,1\prime} = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 1 & 1 \\ 3 & 1 & 2 \end{bmatrix}$	

3 × 3 MDS Matrices

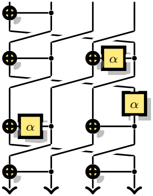
Depth	Cost	M	Fig.
3	5 XOR, 2 LIN	$M_{3,3}^{5,2} = \begin{bmatrix}3 & 1 & 3\\1 & 1 & 2\\2 & 1 & 1\end{bmatrix}$	
2	6 XOR, 3 LIN	$M_{3,2}^{6,3} = \begin{bmatrix}2 & 1 & 1\\1 & 2 & 1\\1 & 1 & 2\end{bmatrix}$	

4 × 4 MDS Matrices

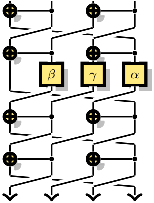
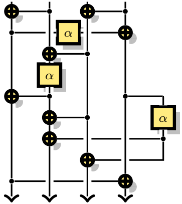
Depth	Cost	Extensions	Memory (GB)	Time (h)
6	8 XOR, 3 LIN		30.9	19.5
5	8 XOR, 3 LIN	`INDEP`	24.3	2.3
5	9 XOR, 3 LIN		154.5	25.6
4	8 XOR, 4 LIN	`MAX_POW` $= 2$	274	30.2
4	9 XOR, 3 LIN	`INDEP`	46	4.5
4	9 XOR, 4 LIN		77.7	12.8
3	9 XOR, 5 LIN	`INV`	279.1	38.5

Table: Optimal 4 × 4 MDS matrices.

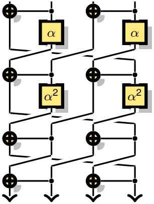
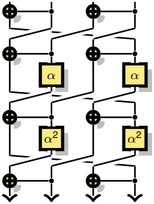
4 × 4 MDS Matrices

Depth	Cost	M	Fig.
6	8 XOR, 3 LIN	$M_{4,6}^{8,3} = \begin{bmatrix} 3 & 1 & 4 & 4 \\ 1 & 3 & 6 & 4 \\ 2 & 2 & 3 & 1 \\ 3 & 2 & 1 & 3 \end{bmatrix}$	

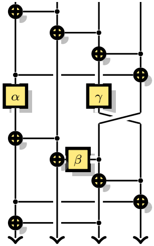
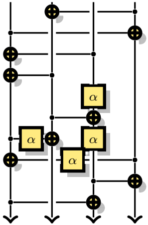
4×4 MDS Matrices

Depth	Cost	M	Fig.
5	8 XOR, 3 LIN	$M_{4,5}^{8,3} = \begin{bmatrix} \alpha+\gamma & \alpha & \gamma & \gamma \\ \alpha+\gamma+1 & \alpha+1 & \gamma+1 & \gamma \\ 1 & 1 & \beta+1 & \beta \\ \gamma+1 & 1 & \beta+\gamma+1 & \beta+\gamma \end{bmatrix}$	
5	9 XOR, 3 LIN	$M_{4,5}^{9,3} = \begin{bmatrix} 2 & 2 & 3 & 1 \\ 1 & 3 & 6 & 4 \\ 3 & 1 & 4 & 4 \\ 3 & 2 & 1 & 3 \end{bmatrix}$	

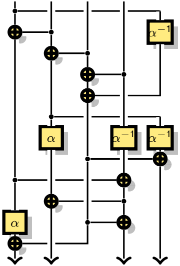
4 × 4 MDS Matrices

Depth	Cost	M	Fig.
4	8 XOR, 4 LIN	$M^{8,4}_{4,4} = \begin{bmatrix} 5 & 7 & 1 & 3 \\ 4 & 6 & 1 & 1 \\ 1 & 3 & 5 & 7 \\ 1 & 1 & 4 & 6 \end{bmatrix}$	
		$M^{8,4\prime}_{4,4} = \begin{bmatrix} 6 & 7 & 1 & 5 \\ 2 & 3 & 1 & 1 \\ 1 & 5 & 6 & 7 \\ 1 & 1 & 2 & 3 \end{bmatrix}$	

4×4 MDS Matrices

Depth	Cost	M	Fig.
4	9 XOR, 3 LIN	$M_{4,4}^{9,3} = \begin{bmatrix} \alpha+1 & \alpha & \gamma+1 & \gamma+1 \\ \beta & \beta+1 & 1 & \beta \\ 1 & 1 & \gamma & \gamma+1 \\ \alpha & \alpha+1 & \gamma+1 & \gamma \end{bmatrix}$	
4	9 XOR, 4 LIN	$M_{4,4}^{9,4} = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 2 & 3 & 2 & 3 \\ 3 & 3 & 5 & 1 \\ 3 & 1 & 1 & 3 \end{bmatrix}$	

4×4 MDS Matrices

Depth	Cost	M	Fig.
3	9 XOR, 5 LIN	$M_{4,3}^{9,5} = \begin{bmatrix} \alpha+\alpha^{-1} & \alpha & 1 & 1 \\ 1 & \alpha+1 & \alpha & \alpha^{-1} \\ 1+\alpha^{-1} & 1 & 1 & 1+\alpha^{-1} \\ \alpha^{-1} & \alpha^{-1} & 1+\alpha^{-1} & 1 \end{bmatrix}$	

From Formal Matrices to Instances

The Idea

1. Input: Formal matrix $M(\alpha)$ MDS
2. Output: $M(A)$ MDS, with A a linear mapping (the lightest we can find)

Characterization of MDS Instantiations

MDS Test

- Intuitive approach:
  1. Choose A a linear mapping
  2. Evaluate $M(A)$
  3. See if all minors are non-zero

Characterization of MDS Instantiations

MDS Test

- Intuitive approach:
  1. Choose A a linear mapping
  2. Evaluate $M(A)$
  3. See if all minors are non-zero
- We can start by computing the minors:
  1. Let I, J subsets of the lines and columns
  2. Define $m_{I,J} = \det_{\mathbb{F}_2[\alpha]}(M_{|I,J})$
  3. $M(A)$ is MDS iff all $m_{I,J}(A)$ are non-zero

Characterization of MDS Instantiations

MDS Test

- Intuitive approach:
  1. Choose A a linear mapping
  2. Evaluate $M(A)$
  3. See if all minors are non-zero
- We can start by computing the minors:
  1. Let I, J subsets of the lines and columns
  2. Define $m_{I,J} = \det_{\mathbb{F}_2[\alpha]}(M_{|I,J})$
  3. $M(A)$ is MDS iff all $m_{I,J}(A)$ are non-zero
- With the minimal polynomial
  1. Let μ_A the minimal polynomial of A
  2. $M(A)$ is MDS iff $\forall(I, J)$, $\gcd(\mu_A, m_{I,J}) = 1$

General Idea of Instantiation

We want A s.t. $\forall(I, J)$, $\gcd(\mu_A, m_{I,J}) = 1$

General Idea of Instantiation

We want A s.t. $\forall(I, J)$, $\gcd(\mu_A, m_{I,J}) = 1$

Easy Way to Instantiate: Multiplications

- $d > \max_{I,J}\{deg(m_{I,J})\}$

General Idea of Instantiation

We want A s.t. $\forall(I,J)$, $\gcd(\mu_A, m_{I,J}) = 1$

Easy Way to Instantiate: Multiplications

- $d > \max_{I,J}\{deg(m_{I,J})\}$
- Choose π an irreducible polynomial of degree d

General Idea of Instantiation

We want A s.t. $\forall(I, J)$, $\gcd(\mu_A, m_{I,J}) = 1$

Easy Way to Instantiate: Multiplications

- $d > \max_{I,J}\{deg(m_{I,J})\}$
- Choose π an irreducible polynomial of degree d
- π is relatively prime with all $m_{I,J}$

General Idea of Instantiation

We want A s.t. $\forall(I, J)$, $\gcd(\mu_A, m_{I,J}) = 1$

Easy Way to Instantiate: Multiplications

- $d > \max_{I,J}\{deg(m_{I,J})\}$
- Choose π an irreducible polynomial of degree d
- π is relatively prime with all $m_{I,J}$
- Take $A =$ companion matrix of π

General Idea of Instantiation

We want A s.t. $\forall(I,J)$, $\gcd(\mu_A, m_{I,J}) = 1$

Easy Way to Instantiate: Multiplications

- $d > \max_{I,J}\{deg(m_{I,J})\}$
- Choose π an irreducible polynomial of degree d
- π is relatively prime with all $m_{I,J}$
- Take $A =$ companion matrix of π
- A corresponds to a finite field multiplication

General Idea of Instantiation

We want A s.t. $\forall(I,J)$, $\gcd(\mu_A, m_{I,J}) = 1$

Easy Way to Instantiate: Multiplications

- $d > \max_{I,J}\{deg(m_{I,J})\}$
- Choose π an irreducible polynomial of degree d
- π is relatively prime with all $m_{I,J}$
- Take $A =$ companion matrix of π
- A corresponds to a finite field multiplication

Low Cost Instantiation

- Pick π with few coefficients: a trinomial requires 1 rotation + 1 binary xor
- If using A^{-1} or A^2, make sure they are lightweight too

Concrete Choices of A

We need to fix the size

Branches of size 4 bits ($\mathbb{F}_{2^4}$)

$$A_4 = \begin{bmatrix} . & 1 & . & . \\ . & . & 1 & . \\ . & . & . & 1 \\ 1 & 1 & . & . \end{bmatrix}$$

(companion matrix of $X^4 + X + 1$ (irreducible))

$$A_4^{-1} = \begin{bmatrix} 1 & . & . & 1 \\ 1 & . & . & . \\ . & 1 & . & . \\ . & . & 1 & . \end{bmatrix}$$

(minimal polynomial is $X^4 + X^3 + 1$)

Branches of size 8 bits ($\mathbb{F}_{2^8}$)

$$A_8 = \begin{bmatrix} . & 1 & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . \\ . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & 1 & . & . \\ . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & . & 1 \\ 1 & . & 1 & . & . & . & . & . \end{bmatrix}$$

(companion matrix of
$X^8 + X^2 + 1 = (X^4 + X + 1)^2$)

$$A_8^{-1} = \begin{bmatrix} . & 1 & . & . & . & . & . & 1 \\ 1 & . & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . \\ . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & 1 & . & . \\ . & . & . & . & . & . & 1 & . \end{bmatrix}$$

(minimal polynomial is $X^8 + X^6 + 1$)

Example of Instantiation: $\mathbb{F}_{2^8}$

In $\mathbb{F}_2^8$, the trinomials and their factorization are

$$\begin{aligned}
X^8 + X \ + 1 &= (X^2 + X + 1)(X^6 + X^5 + X^3 + X^2 + 1),\\
X^8 + X^2 + 1 &= (X^4 + X + 1)^2,\\
X^8 + X^3 + 1 &= (X^3 + X + 1)(X^5 + X^3 + X^2 + X + 1),\\
X^8 + X^4 + 1 &= (X^2 + X + 1)^4,\\
X^8 + X^5 + 1 &= (X^3 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1),\\
X^8 + X^6 + 1 &= (X^4 + X^3 + 1)^2,\\
X^8 + X^7 + 1 &= (X^2 + X + 1)(X^6 + X^4 + X^3 + X + 1).
\end{aligned}$$

In particular, there are only 2 trinomials which factorize to degree 4 polynomials: $X^8 + X^2 + 1 = (X^4 + X + 1)^2$ and $X^8 + X^6 + 1 = (X^4 + X^3 + 1)^2$.

Example of Instantiation: $\mathbb{F}_{2^8}$

In $\mathbb{F}_2^8$, the trinomials and their factorization are

$$\begin{aligned}
X^8 + X \ \ + 1 &= (X^2 + X + 1)(X^6 + X^5 + X^3 + X^2 + 1),\\
X^8 + X^2 + 1 &= (X^4 + X + 1)^2,\\
X^8 + X^3 + 1 &= (X^3 + X + 1)(X^5 + X^3 + X^2 + X + 1),\\
X^8 + X^4 + 1 &= (X^2 + X + 1)^4,\\
X^8 + X^5 + 1 &= (X^3 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1),\\
X^8 + X^6 + 1 &= (X^4 + X^3 + 1)^2,\\
X^8 + X^7 + 1 &= (X^2 + X + 1)(X^6 + X^4 + X^3 + X + 1).
\end{aligned}$$

In particular, there are only 2 trinomials which factorize to degree 4 polynomials: $X^8 + X^2 + 1 = (X^4 + X + 1)^2$ and $X^8 + X^6 + 1 = (X^4 + X^3 + 1)^2$.

Example of Instantiation: $M_{4,6}^{8,3}$

The minors of $M_{4,6}^{8,3} = \begin{bmatrix} 2 & 2 & 3 & 1 \\ 1 & 3 & 6 & 4 \\ 3 & 1 & 4 & 4 \\ 3 & 2 & 1 & 3 \end{bmatrix}$ are

$\{1, X, X+1, X^2, X^2+1, X^2+X, X^2+X+1, X^3, X^3+1, X^3+X, X^3+X+1, X^3+X^2+1, X^3+X^2+X, X^3+X^2+X+1\}$

whose factors are

$$\{X, X+1, X^3+X+1, X^2+X+1, X^3+X^2+1\}$$

On 4 bits: Degrees $\leq 3 \Rightarrow$ relatively prime with X^4+X+1 and X^4+X^3+1 because irreducible
$\alpha = A_4$ or $\alpha = A_4^{-1} \Rightarrow$ MDS matrix over $\mathbb{F}_{2^4}$.

On 8 bits: All relatively prime with X^8+X^2+1 and X^8+X^6+1 ($(X^4+X+1)^2$ and $(X^4+X^3+1)^2$)
$\alpha = A_8$ or $\alpha = A_8^{-1} \Rightarrow$ MDS matrix over $\mathbb{F}_{2^8}$.

Example of Instantiation: $M_{4,4}^{8,4}$

The factors of the minors of $M_{4,4}^{8,4} = \begin{bmatrix} 5 & 7 & 1 & 3 \\ 4 & 6 & 1 & 1 \\ 1 & 3 & 5 & 7 \\ 1 & 1 & 4 & 6 \end{bmatrix}$ are

$$\{X, X+1, X^3+X+1, X^2+X+1, X^3+X^2+1, X^4+X^3+1\}$$

Example of Instantiation: $M_{4,4}^{8,4}$

The factors of the minors of $M_{4,4}^{8,4} = \begin{bmatrix} 5 & 7 & 1 & 3 \\ 4 & 6 & 1 & 1 \\ 1 & 3 & 5 & 7 \\ 1 & 1 & 4 & 6 \end{bmatrix}$ are

$$\{X, X+1, X^3+X+1, X^2+X+1, X^3+X^2+1, X^4+X^3+1\}$$

Factors of degree ≤ 3 relatively prime with X^8+X^2+1 and X^8+X^6+1.

Example of Instantiation: $M_{4,4}^{8,4}$

The factors of the minors of $M_{4,4}^{8,4} = \begin{bmatrix} 5 & 7 & 1 & 3 \\ 4 & 6 & 1 & 1 \\ 1 & 3 & 5 & 7 \\ 1 & 1 & 4 & 6 \end{bmatrix}$ are

$$\{X, X+1, X^3+X+1, X^2+X+1, X^3+X^2+1, X^4+X^3+1\}$$

Factors of degree ≤ 3 relatively prime with X^8+X^2+1 and X^8+X^6+1.

On 4 bits: Not relatively prime with X^4+X^3+1 but all relatively prime with X^4+X+1.
$\alpha = A_4 \Rightarrow$ MDS matrix over $\mathbb{F}_{2^4}$.

Example of Instantiation: $M_{4,4}^{8,4}$

The factors of the minors of $M_{4,4}^{8,4} = \begin{bmatrix} 5 & 7 & 1 & 3 \\ 4 & 6 & 1 & 1 \\ 1 & 3 & 5 & 7 \\ 1 & 1 & 4 & 6 \end{bmatrix}$ are

$$\{X, X+1, X^3+X+1, X^2+X+1, X^3+X^2+1, X^4+X^3+1\}$$

Factors of degree ≤ 3 relatively prime with X^8+X^2+1 and X^8+X^6+1.

On 4 bits: Not relatively prime with X^4+X^3+1 but all relatively prime with X^4+X+1.
$\alpha = A_4 \Rightarrow$ MDS matrix over $\mathbb{F}_{2^4}$.

On 8 bits: Not relatively prime with X^8+X^6+1 but all relatively prime with X^8+X^2+1.
$\alpha = A_8 \Rightarrow$ MDS matrix over $\mathbb{F}_{2^8}$.

Comparison With Existing MDS Matrices

			Cost			
Size	Ring	Matrix	Naive	Best	Depth	Ref
$M_4(M_8(\mathbb{F}_2))$	$GL(8,\mathbb{F}_2)$	Circulant	106			(Li Wang 2016)
	$GL(8,\mathbb{F}_2)$	Hadamard		72	6	(Kranz *et al.* 2018)
	$\mathbb{F}_2[\alpha]$	$M_{4,6}^{8,3}$		67	6	$\alpha = A_8$ or A_8^{-1}
	$\mathbb{F}_2[\alpha]$	$M_{4,5}^{8,3}$		68	5	$\alpha = A_8, \beta = A_8^{-1}, \gamma = A_8^{-2}$
	$\mathbb{F}_2[\alpha]$	$M_{4,4}^{8,4}$		70	4	$\alpha = A_8$
	$\mathbb{F}_2[\alpha]$	$M_{4,3}^{9,5}$		77	3	$\alpha = A_8$ or A_8^{-1}
$M_4(M_4(\mathbb{F}_2))$	$GF(2^4)$	$M_{4,n,4}$	58	58	3	(Jean Peyrin Sim 2017)
	$GF(2^4)$	Toeplitz	58	58	3	(Sarkar Syed 2016)
	$GL(4,\mathbb{F}_2)$	Subfield		36	6	(Kranz *et al.* 2018)
	$\mathbb{F}_2[\alpha]$	$M_{4,6}^{8,3}$		35	6	$\alpha = A_4$ or A_4^{-1}
	$\mathbb{F}_2[\alpha]$	$M_{4,5}^{8,3^{-1}}$		36	5	$\alpha = A_4, \beta = A_4^{-1}, \gamma = A_4^{-2}$
	$\mathbb{F}_2[\alpha]$	$M_{4,4}^{8,4}$		38	4	$\alpha = A_4$
	$\mathbb{F}_2[\alpha]$	$M_{4,3}^{9,5}$		41	3	$\alpha = A_4$ or A_4^{-1}