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**

\[ \mathcal{B}_d(L) = \min_{x \neq 0} \left\{ w(x) + w(L(x)) \right\} \]

**Linear Branch Number**

\[ \mathcal{B}_l(L) = \min_{x \neq 0} \left\{ w(x) + w(L^\top(x)) \right\} \]
SPN Ciphers

Differential Branch Number

\[ B_d(L) = \min_{x \neq 0} \{ w(x) + w(L(x)) \} \]
SPN Ciphers

Differential Branch Number

$$B_d(L) = \min_{x \neq 0} \{ w(x) + w(L(x)) \}$$

Linear Branch Number

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

Maximum branch number: $k + 1$

Can be obtained from MDS codes
Diffusion Matrices

Usually on finite fields:

\[
\begin{bmatrix}
2 & 3 & 1 & 1 \\
1 & 2 & 3 & 1 \\
1 & 1 & 2 & 3 \\
3 & 1 & 1 & 2
\end{bmatrix}
\]

\(x\) 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
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
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

\[
\begin{bmatrix}
3 & 2 & 2 \\
2 & 3 & 2 \\
2 & 2 & 3 \\
\end{bmatrix}
\]

Previous:
\[
\begin{cases}
6 \text{ mult. by 2} \\
3 \text{ mult. by 3} \\
6 \text{ XORS}
\end{cases}
\]

New:
\[
\begin{cases}
1 \text{ mult. by 2} \\
5 \text{ XORS}
\end{cases}
\]
Finite fields $\rightarrow$ polynomial ring

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

**Finite fields → polynomial ring**

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

**Formal matrices**

- $\alpha$ undefined
- $\Rightarrow$ 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 \textit{formal MDS})

Caution: minors are polynomials in $\alpha$

$M(\alpha)$ \textit{formal MDS} $\iff \exists A, M(A)$ 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 $3 \times 3$ and $4 \times 4$

For any word size $n$

Operations:

- word-wise XOR
- $\alpha$ (generalization of a multiplication)
- Copy

$r$ registers: one register per word ($3$ for $3 \times 3$)
+ (at least) one more register $\rightarrow$ 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: $A^*$

**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: $A^*$

Idea of $A^*$
- Guided Dijkstra
- $\text{weight} = \text{weight from origin} + \text{estimated weight to objective}$

Our estimate:
- Heuristic
- How far from MDS?
Optimizations: $A^*$

**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: $A^*$

Idea of $A^*$

- Guided Dijkstra
- \[ \text{weight} = \text{weight from origin} + \text{estimated weight to objective} \]

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: $m = \text{rank of the matrix (without columns containing 0)}$
- 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 $M$: 

- If $M \in \text{TestedNodes}$, skip.
- If $M$ is an MDS matrix, end.
- If $M$ is not an MDS matrix, 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 $M$:
  - $M \in \text{TestedNodes} \rightarrow$ 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 $M$:

- $M \in \text{TestedNodes} \rightarrow \text{skip}$
- MDS? true $\rightarrow$ END
- MDS? false $\rightarrow$ 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 $M$:

- $M \in \text{TestedNodes} \rightarrow \text{skip}$
- MDS? true $\rightarrow$ END
- MDS? false $\rightarrow$ 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 $M$:

- $M \in \text{TestedNodes} \rightarrow$ skip
- MDS? true $\rightarrow$ END
- MDS? false $\rightarrow$ 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

<table>
<thead>
<tr>
<th>Extensions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Additional Read-only Registers</strong></td>
<td>Allow for use of the input values of the function at any time</td>
</tr>
<tr>
<td><strong>Inverse</strong></td>
<td>Allow use of $\alpha^{-1}$</td>
</tr>
<tr>
<td><strong>Powers</strong></td>
<td>Allow use of $\alpha^2$</td>
</tr>
<tr>
<td><strong>Independent Operations</strong></td>
<td>Allow use of 3 independent linear operations $\alpha, \beta, \gamma$</td>
</tr>
</tbody>
</table>
3 × 3 MDS Search

<table>
<thead>
<tr>
<th>Depth</th>
<th>Cost</th>
<th>Extensions</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>5 XOR, 1 LIN</td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>5 XOR, 2 LIN</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>6 XOR, 3 LIN</td>
<td>RO_IN</td>
<td>4</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Depth</th>
<th>Cost</th>
<th>$M$</th>
<th>Fig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>5 XOR, 1 LIN</td>
<td>$M_{3,4}^{5,1} = \begin{bmatrix} 3 &amp; 2 &amp; 2 \ 2 &amp; 3 &amp; 2 \ 2 &amp; 2 &amp; 3 \end{bmatrix}$</td>
<td><img src="image1" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$M_{3,4}^{5,1'} = \begin{bmatrix} 2 &amp; 1 &amp; 3 \ 1 &amp; 1 &amp; 1 \ 3 &amp; 1 &amp; 2 \end{bmatrix}$</td>
<td><img src="image2" alt="Diagram" /></td>
</tr>
</tbody>
</table>

### 3 × 3 MDS Matrices with Lightweight Circuits
### 3 × 3 MDS Matrices

<table>
<thead>
<tr>
<th>Depth</th>
<th>Cost</th>
<th>$M$</th>
<th>Fig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>5 XOR, 2 LIN</td>
<td>$M_{3,3}^{5,2} = \begin{bmatrix} 3 &amp; 1 &amp; 3 \ 1 &amp; 1 &amp; 2 \ 2 &amp; 1 &amp; 1 \end{bmatrix}$</td>
<td><img src="image1.png" alt="Diagram" /></td>
</tr>
<tr>
<td>2</td>
<td>6 XOR, 3 LIN</td>
<td>$M_{3,2}^{6,3} = \begin{bmatrix} 2 &amp; 1 &amp; 1 \ 1 &amp; 2 &amp; 1 \ 1 &amp; 1 &amp; 2 \end{bmatrix}$</td>
<td><img src="image2.png" alt="Diagram" /></td>
</tr>
</tbody>
</table>
### 4 × 4 MDS Matrices

<table>
<thead>
<tr>
<th>Depth</th>
<th>Cost</th>
<th>Extensions</th>
<th>Memory (GB)</th>
<th>Time (h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>8 XOR, 3 LIN</td>
<td></td>
<td>30.9</td>
<td>19.5</td>
</tr>
<tr>
<td>5</td>
<td>8 XOR, 3 LIN</td>
<td>INDEP</td>
<td>24.3</td>
<td>2.3</td>
</tr>
<tr>
<td>5</td>
<td>9 XOR, 3 LIN</td>
<td></td>
<td>154.5</td>
<td>25.6</td>
</tr>
<tr>
<td>4</td>
<td>8 XOR, 4 LIN</td>
<td>MAX_POW = 2</td>
<td>274</td>
<td>30.2</td>
</tr>
<tr>
<td>4</td>
<td>9 XOR, 3 LIN</td>
<td>INDEP</td>
<td>46</td>
<td>4.5</td>
</tr>
<tr>
<td>4</td>
<td>9 XOR, 4 LIN</td>
<td></td>
<td>77.7</td>
<td>12.8</td>
</tr>
<tr>
<td>3</td>
<td>9 XOR, 5 LIN</td>
<td>INV</td>
<td>279.1</td>
<td>38.5</td>
</tr>
</tbody>
</table>

**Table:** Optimal 4 × 4 MDS matrices.
### 4 × 4 MDS Matrices

<table>
<thead>
<tr>
<th>Depth</th>
<th>Cost</th>
<th>$M$</th>
<th>Fig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>8 XOR, 3 LIN</td>
<td>$M_{4,6}^{8,3} = \begin{bmatrix} 3 &amp; 1 &amp; 4 &amp; 4 \ 1 &amp; 3 &amp; 6 &amp; 4 \ 2 &amp; 2 &amp; 3 &amp; 1 \ 3 &amp; 2 &amp; 1 &amp; 3 \end{bmatrix}$</td>
<td><img src="#" alt="Diagram" /></td>
</tr>
</tbody>
</table>
### 4 × 4 MDS Matrices

<table>
<thead>
<tr>
<th>Depth</th>
<th>Cost</th>
<th>$M$</th>
<th>Fig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>8 XOR, 3 LIN</td>
<td>$M_{4,5}^{8,3} = \begin{bmatrix} \alpha + \gamma &amp; \alpha &amp; \gamma &amp; \gamma \ \alpha + \gamma + 1 &amp; \alpha + 1 &amp; \gamma + 1 &amp; \gamma \ 1 &amp; 1 &amp; \beta + 1 &amp; \beta \ \gamma + 1 &amp; 1 &amp; \beta + \gamma + 1 &amp; \beta + \gamma \end{bmatrix}$</td>
<td><img src="image1.png" alt="Diagram 1" /></td>
</tr>
<tr>
<td>5</td>
<td>9 XOR, 3 LIN</td>
<td>$M_{4,5}^{9,3} = \begin{bmatrix} 2 &amp; 2 &amp; 3 &amp; 1 \ 1 &amp; 3 &amp; 6 &amp; 4 \ 3 &amp; 1 &amp; 4 &amp; 4 \ 3 &amp; 2 &amp; 1 &amp; 3 \end{bmatrix}$</td>
<td><img src="image2.png" alt="Diagram 2" /></td>
</tr>
</tbody>
</table>
### 4 × 4 MDS Matrices

<table>
<thead>
<tr>
<th>Depth</th>
<th>Cost</th>
<th>$M$</th>
<th>Fig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>8 XOR, 4 LIN</td>
<td>$M_{4,4}^{8,4} = \begin{bmatrix} 5 &amp; 7 &amp; 1 &amp; 3 \ 4 &amp; 6 &amp; 1 &amp; 1 \ 1 &amp; 3 &amp; 5 &amp; 7 \ 1 &amp; 1 &amp; 4 &amp; 6 \end{bmatrix}$</td>
<td>![Diagram 1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$M_{4,4}^{8,4'} = \begin{bmatrix} 6 &amp; 7 &amp; 1 &amp; 5 \ 2 &amp; 3 &amp; 1 &amp; 1 \ 1 &amp; 5 &amp; 6 &amp; 7 \ 1 &amp; 1 &amp; 2 &amp; 3 \end{bmatrix}$</td>
<td>![Diagram 2]</td>
</tr>
</tbody>
</table>

## 4 × 4 MDS Matrices

<table>
<thead>
<tr>
<th>Depth</th>
<th>Cost</th>
<th>$M$</th>
<th>Fig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>9 XOR, 3 LIN</td>
<td>$M_{4,4}^{9,3} = \begin{bmatrix} \alpha + 1 &amp; \alpha &amp; \gamma + 1 &amp; \gamma + 1 \ \beta &amp; \beta + 1 &amp; 1 &amp; \beta \ 1 &amp; 1 &amp; \gamma &amp; \gamma + 1 \ \alpha &amp; \alpha + 1 &amp; \gamma + 1 &amp; \gamma \end{bmatrix}$</td>
<td><img src="image1.png" alt="Diagram" /></td>
</tr>
<tr>
<td>4</td>
<td>9 XOR, 4 LIN</td>
<td>$M_{4,4}^{9,4} = \begin{bmatrix} 1 &amp; 2 &amp; 4 &amp; 3 \ 2 &amp; 3 &amp; 2 &amp; 3 \ 3 &amp; 3 &amp; 5 &amp; 1 \ 3 &amp; 1 &amp; 1 &amp; 3 \end{bmatrix}$</td>
<td><img src="image2.png" alt="Diagram" /></td>
</tr>
</tbody>
</table>
### 4 × 4 MDS Matrices

<table>
<thead>
<tr>
<th>Depth</th>
<th>Cost</th>
<th>( M )</th>
<th>Fig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>9 XOR, 5 LIN</td>
<td>( M_{4,3}^{9,5} = \begin{bmatrix} \alpha + \alpha^{-1} &amp; \alpha &amp; 1 &amp; 1 \ 1 &amp; \alpha + 1 &amp; \alpha &amp; \alpha^{-1} \ 1 + \alpha^{-1} &amp; 1 &amp; 1 + \alpha^{-1} &amp; 1 \end{bmatrix} )</td>
<td><img src="image" alt="Diagram" /></td>
</tr>
</tbody>
</table>
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 $\mu_A$ the minimal polynomial of $A$
  2. $M(A)$ is MDS iff $\forall (I, J), \gcd(\mu_A, m_{I,J}) = 1$
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 $\pi$ 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**

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

Low Cost Instantiation

- Pick $\pi$ 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 ($\mathbb{F}_{2^4}$)

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

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

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

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

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

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

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

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

(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

\[
X^8 + X + 1 = (X^2 + X + 1)(X^6 + X^5 + X^3 + X^2 + 1),
\]
\[
X^8 + X^2 + 1 = (X^4 + X + 1)^2,
\]
\[
X^8 + X^3 + 1 = (X^3 + X + 1)(X^5 + X^3 + X^2 + X + 1),
\]
\[
X^8 + X^4 + 1 = (X^2 + X + 1)^4,
\]
\[
X^8 + X^5 + 1 = (X^3 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1),
\]
\[
X^8 + X^6 + 1 = (X^4 + X^3 + 1)^2,
\]
\[
X^8 + X^7 + 1 = (X^2 + X + 1)(X^6 + X^4 + X^3 + X + 1).
\]

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

\[
\begin{align*}
X^8 + X + 1 &= (X^2 + X + 1)(X^6 + X^5 + X^3 + X^2 + 1), \\
X^8 + X^2 + 1 &= (X^4 + X + 1)^2, \\
X^8 + X^3 + 1 &= (X^3 + X + 1)(X^5 + X^3 + X^2 + X + 1), \\
X^8 + X^4 + 1 &= (X^2 + X + 1)^4, \\
X^8 + X^5 + 1 &= (X^3 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1), \\
X^8 + X^6 + 1 &= (X^4 + X^3 + 1)^2, \\
X^8 + X^7 + 1 &= (X^2 + X + 1)(X^6 + X^4 + X^3 + X + 1).
\end{align*}
\]

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

S. Duval, G. Leurent
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 $\leq 3$ 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 $\leq 3$ 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 $\leq 3$ 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

<table>
<thead>
<tr>
<th>Size</th>
<th>Ring</th>
<th>Matrix</th>
<th>Cost</th>
<th>Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_4(M_8(\mathbb{F}_2))$</td>
<td>$GL(8, \mathbb{F}_2)$</td>
<td>Circulant</td>
<td>106</td>
<td>(Li Wang 2016)</td>
</tr>
<tr>
<td>$GL(8, \mathbb{F}_2)$</td>
<td></td>
<td></td>
<td></td>
<td>(Kranz et al. 2018)</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td></td>
<td>$M_{4,6}^{3,3}$</td>
<td>67</td>
<td>$\alpha = A_8$ or $A_8^{-1}$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td></td>
<td>$M_{4,5}^{3,3}$</td>
<td>68</td>
<td>$\alpha = A_8, \beta = A_8^{-1}, \gamma = A_8^{-2}$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td></td>
<td>$M_{4,4}^{3,4}$</td>
<td>70</td>
<td>$\alpha = A_8$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td></td>
<td>$M_{4,3}^{3,5}$</td>
<td>77</td>
<td>$\alpha = A_8$ or $A_8^{-1}$</td>
</tr>
<tr>
<td>$M_4(M_4(\mathbb{F}_2))$</td>
<td>$GF(2^4)$</td>
<td>$M_{4,n,4}$</td>
<td>58</td>
<td>(Jean Peyrin Sim 2017)</td>
</tr>
<tr>
<td>$GF(2^4)$</td>
<td></td>
<td></td>
<td>58</td>
<td>(Sarkar Syed 2016)</td>
</tr>
<tr>
<td>$GL(4, \mathbb{F}_2)$</td>
<td></td>
<td>Subfield</td>
<td>36</td>
<td>(Kranz et al. 2018)</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td></td>
<td>$M_{4,6}^{3,3}$</td>
<td>35</td>
<td>$\alpha = A_4$ or $A_4^{-1}$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td></td>
<td>$M_{4,5}^{3,3}^{-1}$</td>
<td>36</td>
<td>$\alpha = A_4, \beta = A_4^{-1}, \gamma = A_4^{-2}$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td></td>
<td>$M_{4,4}^{3,4}$</td>
<td>38</td>
<td>$\alpha = A_4$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td></td>
<td>$M_{4,3}^{3,5}$</td>
<td>41</td>
<td>$\alpha = A_4$ or $A_4^{-1}$</td>
</tr>
</tbody>
</table>