MDS Matrices with Lightweight Circuits

Sébastien Duval  
Gaëtan Leurent

March 26, 2019
**SPN 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

**Example:** Rijndael/AES [Daemen Rijmen 1998]
Block Cipher Security Analysis

Differential Attacks [Biham Shamir 91]

- Attacker exploits \((a, b)\) such that
  \[ E_K(x) \oplus E_K(x \oplus a) = b \]
  with high probability
- Maximum of the probability over all \((a, b)\) bounded by
  \[ \left( \frac{\delta(S)}{2^n} \right) B_d(L) - 1 \]
MDS Matrices

Differential Branch Number

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

where \( w(x) \) is the number of non-zero \( n \)-bits words in \( x \).

Linear Branch Number

\[ B_l(L) = \min_{x \neq 0} \{ w(x) + w(L^T(x)) \} \]
MDS Matrices

**Differential Branch Number**

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

where \( w(x) \) is the number of non-zero \( n \)-bits words in \( x \).

**Linear Branch Number**

\[ B_l(L) = \min_{x \neq 0} \{ w(x) + w(L^T(x)) \} \]

Maximum branch number: \( k + 1 \)

Equivalent to MDS codes.

---

\[ L \text{ linear permutation on } k \text{ words of } n \text{ bits.} \]
MDS Matrices

Differential Branch Number

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

where $w(x)$ is the number of non-zero $n$-bits words in $x$.

Linear Branch Number

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

Maximum branch number: $k + 1$

Equivalent to MDS codes.

$L$ linear permutation on $k$ words of $n$ bits.
Matrices and Characterisation

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

AES MixColumns

Usually on finite fields:
- $x$ a primitive element of $\mathbb{F}_2^n$
- Coeffs. $\in \mathbb{F}_2[x]/P$, with $P$ a primitive polynomial
- $2 \leftrightarrow x$
- $3 \leftrightarrow x + 1$

Characterisation

$L$ is MDS iff its minors are non-zero
Previous Works

Recursive Matrices [Guo et al. 2011]

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: inputs are binary vectors, matrix coeffs. are $n \times n$ matrices.

$\Rightarrow$ less costly operations than multiplication in a finite field
Cost Evaluation

“Real cost”
Number of operations of the best implementation.

Xor count (naive cost)
Hamming weight of the binary matrix. Cannot reuse intermediate values.

Intermediate values

- Local optimisation: LIGHTER [Jean et al. 2017]
  cost of matrix multiplication = number of XORs + cost of the mult. by each coefficient.

- Global optimisation:
  - Our approach: Number of operations of the best implementation using operations on words.
Metrics Comparison

Xor Count: \[
\begin{bmatrix}
3 & 2 & 2 \\
2 & 3 & 2 \\
2 & 2 & 3
\end{bmatrix}
\]

\[
\times 2
\]

Our approach:
\[
\begin{aligned}
& 1 \text{ mult. by 2} \\
& 5 \text{ XORS}
\end{aligned}
\]

6 mult. by 2
3 mult. by 3
6 XORS
Formal Matrices

Formal matrices

- Optimise in 2 steps:
  1. Find $M(\alpha)$ for $\alpha$ an undefined linear mapping.
  2. Instantiate with the best choice of $\alpha$

- Not necessarily a finite field.
- Then coeffs. are polynomials in $\alpha$.

\[
\begin{bmatrix}
\alpha + 1 & \alpha & \alpha \\
\alpha & \alpha + 1 & \alpha \\
\alpha & \alpha & \alpha + 1
\end{bmatrix}
\]
Formal Matrices

Formal matrices

- Optimise in 2 steps:
  1. Find $M(\alpha)$ for $\alpha$ an undefined linear mapping.
  2. Instantiate with the best choice of $\alpha$.
- Not necessarily a finite field.
- Then coeffs. are polynomials in $\alpha$.

Characterisation of formally MDS matrices

- Objective: find $M(\alpha)$ s.t. $\exists A$, $M(A)$ MDS.
- If a minor of $M(\alpha)$ is null, then impossible.
- Otherwise, there always exists an $A$.

Characterisation possible on $M(\alpha)$. 

\[
\begin{bmatrix}
\alpha+1 & \alpha & \alpha \\
\alpha & \alpha+1 & \alpha \\
\alpha & \alpha & \alpha+1
\end{bmatrix}
\]
Search over circuits

Search Space

Operations:

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

Note: Only word-wise operations.

$r$ registers:
- one register per word ($3$ for $3 \times 3$)
- $+$ (at least) one more register $\rightarrow$ more complex operations
Implementation: Main Idea

Tree-based Dijkstra search

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

Search results

- $k = 3$ fast (seconds)
- $k = 4$ long (hours)
- $k = 5$ out of reach
- Collection of MDS matrices with trade-off between cost and depth (latency).
Scheme of the Search
Optimization: $A^*$

**A***

Idea of $A^*$

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

**A***

Idea of $A^*$

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

Our estimate:
Optimization: $A^*$

**A***

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

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

**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
Optimization: \( A^* \)

### 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
Optimization: $A^*$

**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
- Estimate: $m = \text{rank of the matrix (without columns containing 0)}$
- Need at least $k - m$ word-wise XORs to MDS

Result: much faster
Methodology of the Instantiation

The Idea

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

**MDS Test**

- Intuitive approach:
  - Choose $A$ a linear mapping
  - Evaluate $M(A)$
  - See if all minors are non-singular
Characterisation of MDS Instantiations

MDS Test

- **Intuitive approach:**
  - Choose $A$ a linear mapping
  - Evaluate $M(A)$
  - See if all minors are non-singular

- We can start by computing the minors:
  - Let $I, J$ subsets of the lines and columns
  - Define $m_{I,J} = \det_{F_2^{|\alpha|}}(M_{|I,J})$
  - $M(A)$ is MDS iff all $m_{I,J}(A)$ are non-singular
Characterisation of MDS Instantiations

**MDS Test**

- **Intuitive approach:**
  - Choose $A$ a linear mapping
  - Evaluate $M(A)$
  - See if all minors are non-singular

- **We can start by computing the minors:**
  - Let $I, J$ subsets of the lines and columns
  - Define $m_{I,J} = \text{det}_{\mathbb{F}_2[\alpha]}(M|_{I,J})$
  - $M(A)$ is MDS iff all $m_{I,J}(A)$ are non-singular

- **With the minimal polynomial**
  - Let $\mu_A$ the minimal polynomial of $A$
  - $M(A)$ is MDS iff $\forall (I, J), \gcd(\mu_A, m_{I,J}) = 1$
Multiplications in a Finite Field

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

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

Easy Way to Instantiate: Multiplications

- $d > \max_{I,J}\{\deg(m_{I,J})\}$
Multiplications in a Finite Field

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 $d$
Multiplications in a Finite Field

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 $m_{I,J}$
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 $A = \text{companion matrix of } \pi$
Multiplications in a Finite Field

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 $A = \text{companion matrix} \text{ of } \pi$
- $A$ corresponds to a finite field multiplication
Multiplications in a Finite Field

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
Concrete Choices of $A$

We need to fix the size

Branches of size 4 bits ($\mathbb{F}_2^4$)

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

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

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

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

Branches of size 8 bits ($\mathbb{F}_2^8$)

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

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

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

(minimal polynomial is $X^8 + X^6 + 1$)
### Comparison With Existing MDS Matrices

<table>
<thead>
<tr>
<th>Size</th>
<th>Ring</th>
<th>Matrix</th>
<th>Cost</th>
<th>Naive</th>
<th>Best</th>
<th>Depth</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></td>
<td></td>
<td></td>
<td>(Li Wang 2016)</td>
</tr>
<tr>
<td></td>
<td>$GL(8, \mathbb{F}_2)$</td>
<td>Hadamard</td>
<td></td>
<td>72</td>
<td></td>
<td>6</td>
<td>(Kranz et al. 2018)</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td>$M_8^{8,3}$</td>
<td></td>
<td>67</td>
<td>5</td>
<td></td>
<td></td>
<td>$\alpha = A_8$ or $A_8^{-1}$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td>$M_8^{8,4}$</td>
<td></td>
<td>69</td>
<td>4</td>
<td></td>
<td></td>
<td>$\alpha = A_8$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td>$M_9^{9,5}$</td>
<td></td>
<td>77</td>
<td>3</td>
<td></td>
<td></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>58</td>
<td></td>
<td>3</td>
<td>(Jean Peyrin Sim 2017)</td>
</tr>
<tr>
<td></td>
<td>$GF(2^4)$</td>
<td>Toeplitz</td>
<td>58</td>
<td>58</td>
<td></td>
<td>3</td>
<td>(Sarkar Syed 2016)</td>
</tr>
<tr>
<td></td>
<td>$GL(4, \mathbb{F}_2)$</td>
<td>Subfield</td>
<td>36</td>
<td>36</td>
<td></td>
<td>6</td>
<td>(Kranz et al. 2018)</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td>$M_8^{8,3}$</td>
<td></td>
<td>35</td>
<td>5</td>
<td></td>
<td></td>
<td>$\alpha = A_4$ or $A_4^{-1}$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td>$M_8^{8,4}$</td>
<td></td>
<td>37</td>
<td>4</td>
<td></td>
<td></td>
<td>$\alpha = A_4$</td>
</tr>
<tr>
<td>$\mathbb{F}_2[\alpha]$</td>
<td>$M_9^{9,5}$</td>
<td></td>
<td>41</td>
<td>3</td>
<td></td>
<td></td>
<td>$\alpha = A_4$ or $A_4^{-1}$</td>
</tr>
</tbody>
</table>