RUHR-UNIVERSITÄT BOCHUM

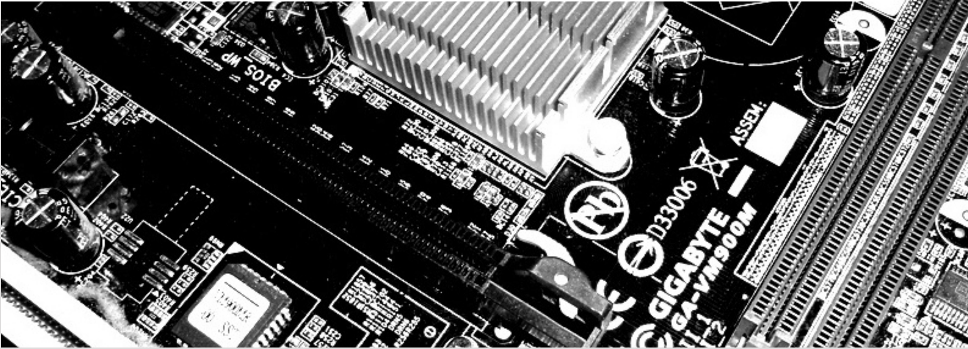
XOR Count

October XXth, 2017

FluxFingers

Workgroup Symmetric Cryptography
Ruhr University Bochum

Friedrich Wiemer



Overview

Joint Work – Its not me alone

Thorsten Kranz, Gregor Leander, Ko Stoffelen, Friedrich Wiemer

RUHR UNIVERSITÄT BOCHUM RUB

Radboud University

Outline

1. Motivation
2. Preliminaries
3. State of the Art and Related Work
4. Future Work

What is the XOR count,
and why is it important?

Some facts

- Lightweight Block Ciphers
- Efficient Linear Layers
- MDS matrices are “optimal” (regarding security)[1]

[1] Are they?

What is the XOR count,
and why is it important?

Some facts

- Lightweight Block Ciphers
- Efficient Linear Layers
- MDS matrices are “optimal” (regarding security)[1]
- What is the lightest implementable MDS matrix?
- What about additional features (Involutory)?

[1] Are they?

What is the XOR count,
and why is it important?

Some facts

- Lightweight Block Ciphers
- Efficient Linear Layers
- MDS matrices are “optimal” (regarding security)[1]
- What is the lightest implementable MDS matrix?
- What about additional features (Involutory)?

The XOR count

- Metric for needed hardware resources
- Smaller is better

[1] Are they?

What is an MDS matrix?

RUB

Definition: MDS

A matrix M of dimension k over the field $\mathbb{F}$ is *maximum distance separable* (MDS), iff all possible submatrices of M are invertible (or nonsingular).

What is an MDS matrix?

RUB

Definition: MDS

A matrix M of dimension k over the field $\mathbb{F}$ is *maximum distance separable* (MDS), iff all possible submatrices of M are invertible (or nonsingular).

Example

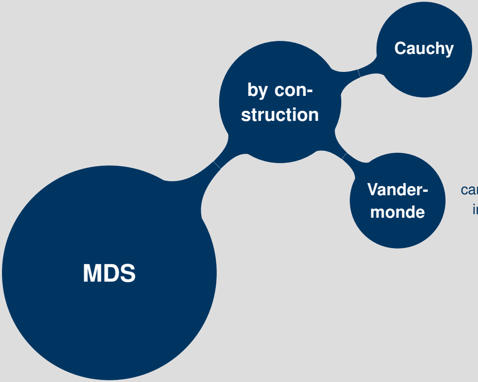
The AES MixColumn matrix is defined over $\mathbb{F}_{2^8} \cong \mathbb{F}[x]/\mathtt{0x11b}$:

$$\begin{pmatrix} \mathtt{0x02} & \mathtt{0x03} & \mathtt{0x01} & \mathtt{0x01} \\ \mathtt{0x01} & \mathtt{0x02} & \mathtt{0x03} & \mathtt{0x01} \\ \mathtt{0x01} & \mathtt{0x01} & \mathtt{0x02} & \mathtt{0x03} \\ \mathtt{0x03} & \mathtt{0x01} & \mathtt{0x01} & \mathtt{0x02} \end{pmatrix} = \begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix}$$

This is a (right) *circulant* matrix: $\mathrm{circ}(x, x+1, 1, 1)$.

What is an MDS matrix?

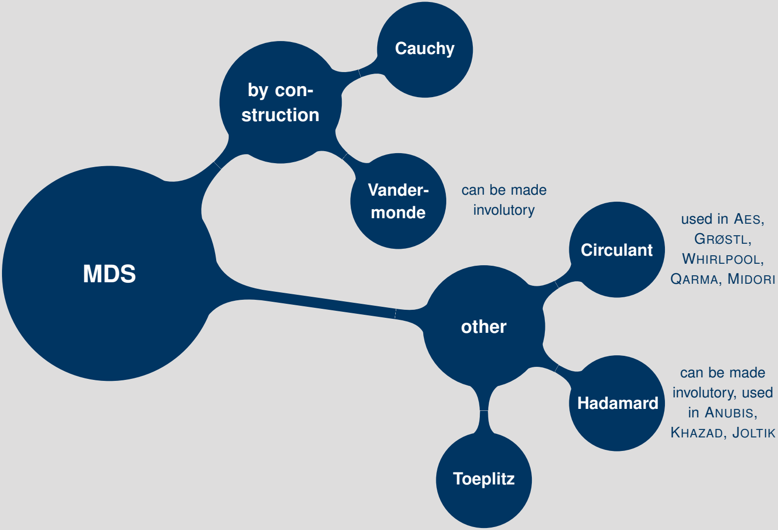
Constructions



can be made involutory

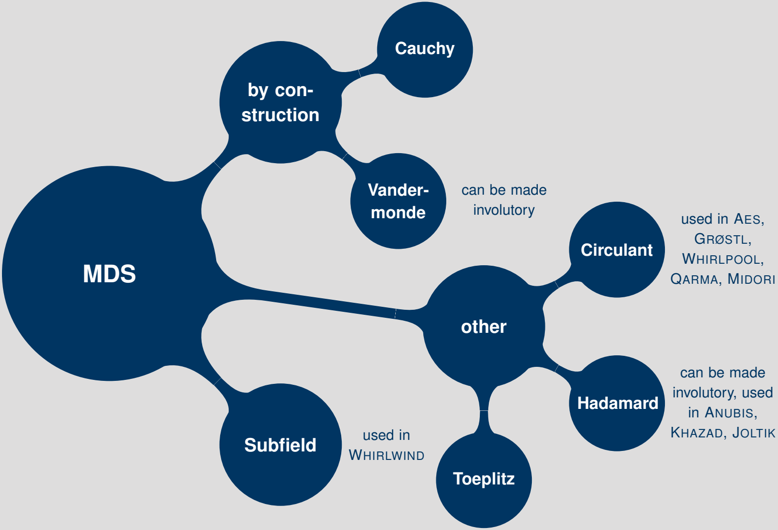
What is an MDS matrix?

Constructions



What is an MDS matrix?

Constructions



What is an MDS matrix?

Representations

How to implement this in hardware?

- This is about hardware implementations
- How do we implement a field multiplication in hardware?
- How do we implement a matrix multiplication in hardware?

What is an MDS matrix?

Representations

How to implement this in hardware?

- This is about hardware implementations
- How do we implement a *field multiplication* in hardware?
- How do we implement a matrix multiplication in hardware?

Example

$$\alpha \longrightarrow \boxed{\cdot 1} \longrightarrow \beta \qquad \alpha \longrightarrow \boxed{\cdot x} \longrightarrow \beta \qquad \alpha \longrightarrow \boxed{\cdot (x+1)} \longrightarrow \beta$$

What is an MDS matrix?

Representations

How to implement this in hardware?

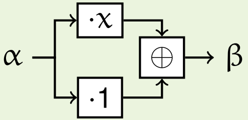
- This is about hardware implementations
- How do we implement a *field multiplication* in hardware?
- How do we implement a matrix multiplication in hardware?

Example

$$\alpha \rightarrow \boxed{\cdot 1} \rightarrow \beta$$

$$\alpha \rightarrow \boxed{\cdot x} \rightarrow \beta$$

$$\alpha \rightarrow \boxed{\cdot (x+1)} \rightarrow \beta$$



Field Multiplication in Hardware

From $\mathbb{F}_2[x]/p(x)$ to $\mathbb{F}_2^n$

RUB

Implement $\alpha \longrightarrow \boxed{\cdot 1} \longrightarrow \beta$

OK, this one is easy ☺

Example in $\mathbb{F}_2[x]/0x13$:

Field Multiplication in Hardware

From $\mathbb{F}_2[x]/p(x)$ to $\mathbb{F}_2^n$

Implement $\alpha \longrightarrow \boxed{\cdot 1} \longrightarrow \beta$

OK, this one is easy ☺

Example in $\mathbb{F}_2[x]/0x13$:

$$\begin{aligned}\alpha &= \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 \\ \beta &= \beta_0 + \beta_1 x + \beta_2 x^2 + \beta_3 x^3 \\ &= \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3\end{aligned}$$

Field Multiplication in Hardware

From $\mathbb{F}_2[x]/p(x)$ to $\mathbb{F}_2^n$

Implement $\alpha \longrightarrow \boxed{\cdot x} \longrightarrow \beta$

Example in $\mathbb{F}_2[x]/0x13$:

Field Multiplication in Hardware

From $\mathbb{F}_2[x]/p(x)$ to $\mathbb{F}_2^n$

RUB

Implement $\alpha \rightarrow \boxed{\cdot x} \rightarrow \beta$

Example in $\mathbb{F}_2[x]/$0x13:

$$\begin{aligned} \alpha &= \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 \\ x^4 &\equiv x + 1 \bmod \text{0x13} \\ \beta &= \beta_0 + \beta_1 x + \beta_2 x^2 + \beta_3 x^3 \\ &= x \cdot (\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3) \\ &\equiv \alpha_3 + (\alpha_0 + \alpha_3)x + \alpha_1 x^2 + \alpha_2 x^3) \end{aligned}$$

Field Multiplication in Hardware

From $\mathbb{F}_2[x]/p(x)$ to $\mathbb{F}_2^n$

In matrix notation for $\mathbb{F}_2[x]/0x13$:

$$\beta = 1 \cdot \alpha \Leftrightarrow \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$$

$$\beta = x \cdot \alpha \Leftrightarrow \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$$

Field Multiplication in Hardware

From $\mathbb{F}_2[x]/p(x)$ to $\mathbb{F}_2^n$

RUB

In matrix notation for $\mathbb{F}_2[x]/0x13$:

$$\beta = 1 \cdot \alpha \Leftrightarrow \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$$

$$\beta = x \cdot \alpha \Leftrightarrow \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$$

Companion Matrix

We call $M_{p(x)} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ the *companion matrix* of the polynomial $p(x) = 0x13$. For any element $\gamma \in \mathbb{F}_2[x]/p(x)$, we denote by M_γ the matrix that implements the multiplication by this element in $\mathbb{F}_2^n$.

Counting XOR's

Example

We can rewrite the AES MIXCOLUMN matrix as:

$$\mathcal{M}_{\text{AES}} = \text{circ}(x, x+1, 1, 1) \cong \text{circ}(M_x, M_{x+1}, M_1, M_1).$$

Starting in $(\mathbb{F}_2[x]/\text{0x11b})^{4\times 4}$, we end up in $\left({\mathbb{F}_2}^{8\times 8}\right)^{4\times 4} \cong \mathbb{F}_2^{32\times 32}$.

Counting XOR's

Example

We can rewrite the AES MIXCOLUMN matrix as:

$$\mathcal{M}_{\text{AES}} = \text{circ}(x, x+1, 1, 1) \cong \text{circ}(M_x, M_{x+1}, M_1, M_1).$$

Starting in $(\mathbb{F}_2[x]/\text{0x11b})^{4\times 4}$, we end up in $\left({\mathbb{F}_2}^{8\times 8}\right)^{4\times 4} \cong \mathbb{F}_2^{32\times 32}$.

A first XOR-count

To implement multiplication by γ, we need $\text{hw}(M_\gamma) - \dim(M_\gamma)$ many XOR's. Thus

$$\begin{aligned} \text{XOR-count}(\mathcal{M}_{\text{AES}}) &= 4 \cdot (\text{hw}(M_x) + \text{hw}(M_{x+1}) + 2 \cdot \text{hw}(M_1)) - 32 \\ &= 4 \cdot (11 + 19 + 2 \cdot 8) - 32 = 152. \end{aligned}$$

The General Linear Group

Generalise a bit

Instead of choosing elements from $\mathbb{F}_{2^n} \cong \mathbb{F}_2[x]/p(x)$ we can extend our possible choices for "multiplication matrices" by exploiting the following.

The General Linear Group

Generalise a bit

Instead of choosing elements from $\mathbb{F}_{2^n} \cong \mathbb{F}_2[x]/p(x)$ we can extend our possible choices for “multiplication matrices” by exploiting the following.

Todo

Maybe remove this?

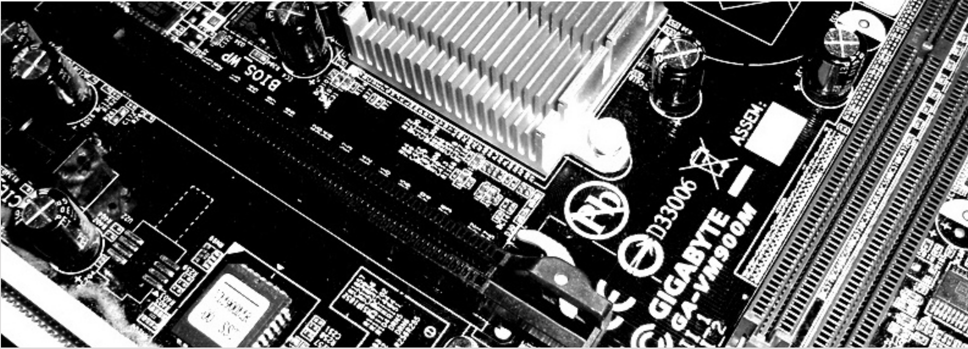
The Stupidity of recent XOR Count Papers

October XXth, 2017

FluxFingers

Workgroup Symmetric Cryptography
Ruhr University Bochum

Friedrich Wiemer



State of the Art

Before our Paper

Related Work I

Related Work II

State of the Art

After our Paper

Future Work

Questions?

Thank you for your attention!

Mainboard & Questionmark Images: flickr

References I