RUHR-UNIVERSITÄT BOCHUM

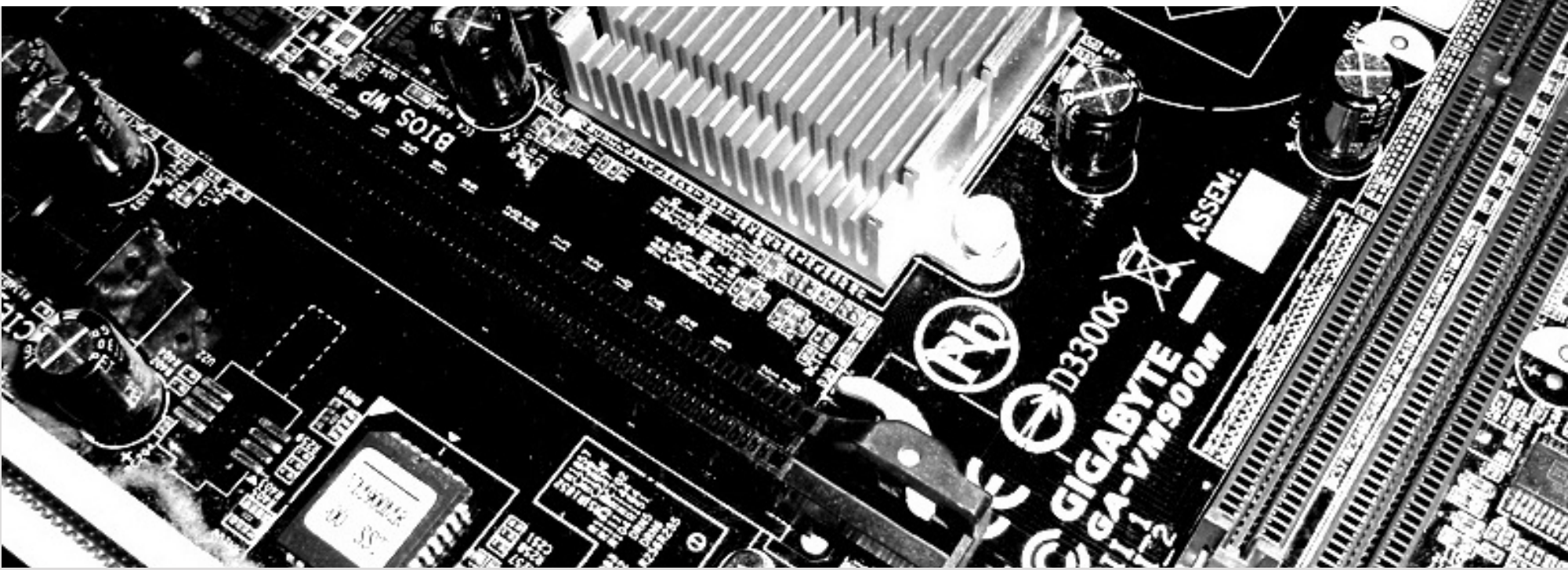
XOR Count

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

What is the XOR count,

and why is it important?

RUB

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?

RUB

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 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

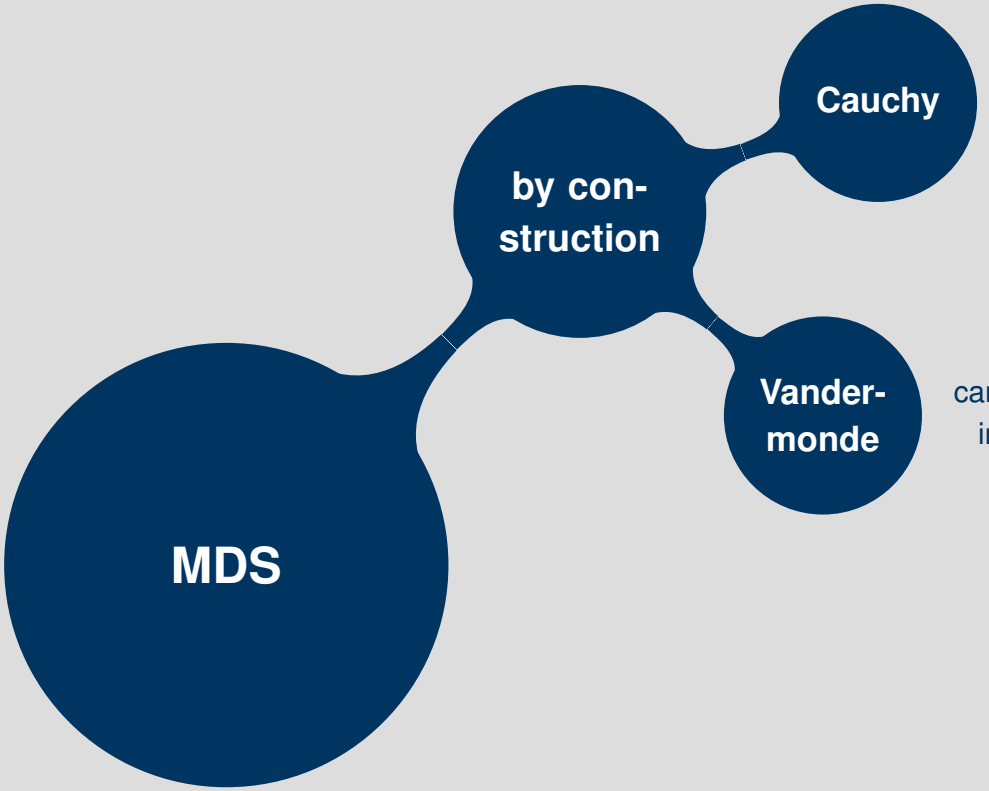
The AES MIXCOLUMN matrix is defined over $\mathbb{F}_{2^8} \cong \mathbb{F}[\mathrm{x}]/\mathtt{0x11b}$:

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

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

What is an MDS matrix?

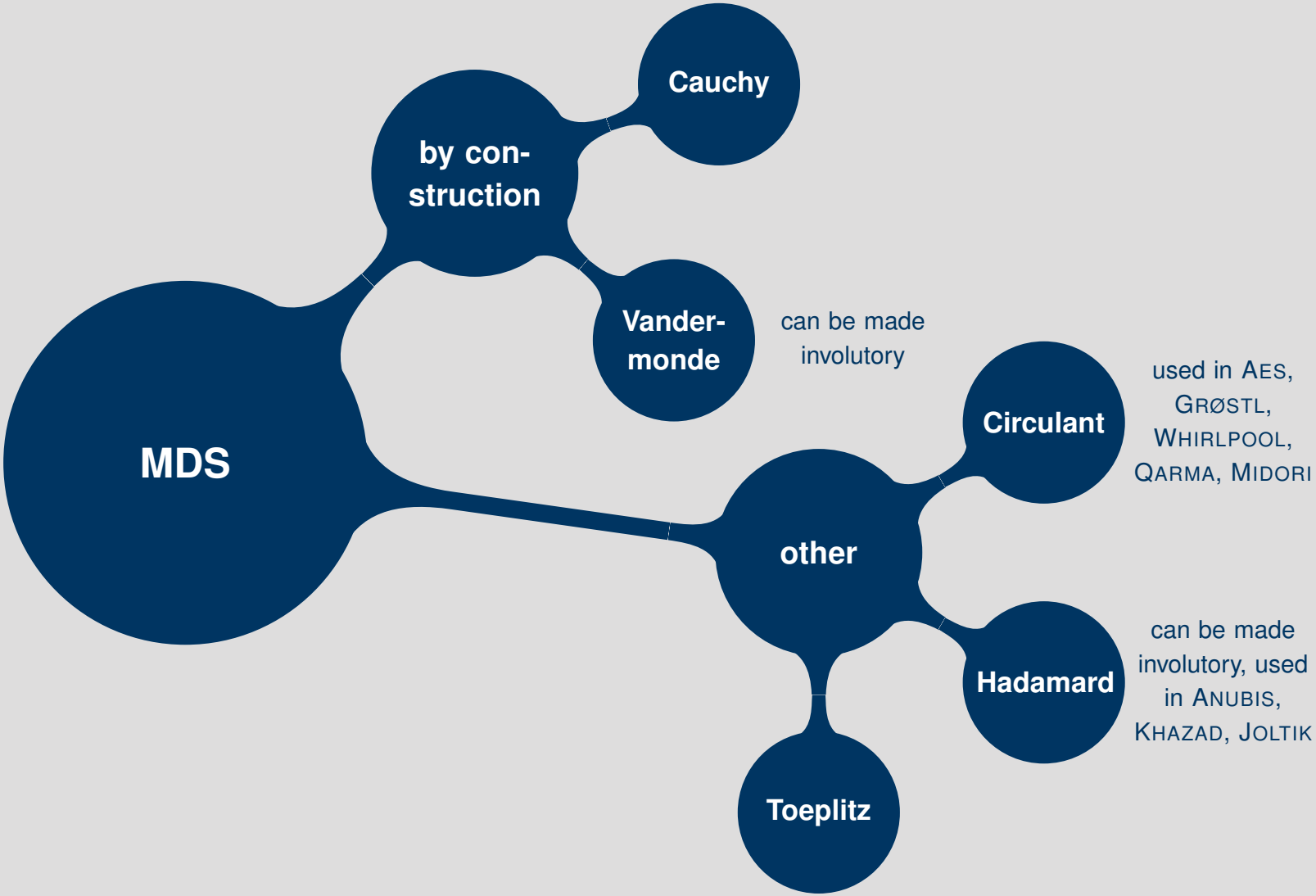
Constructions



can be made involutory

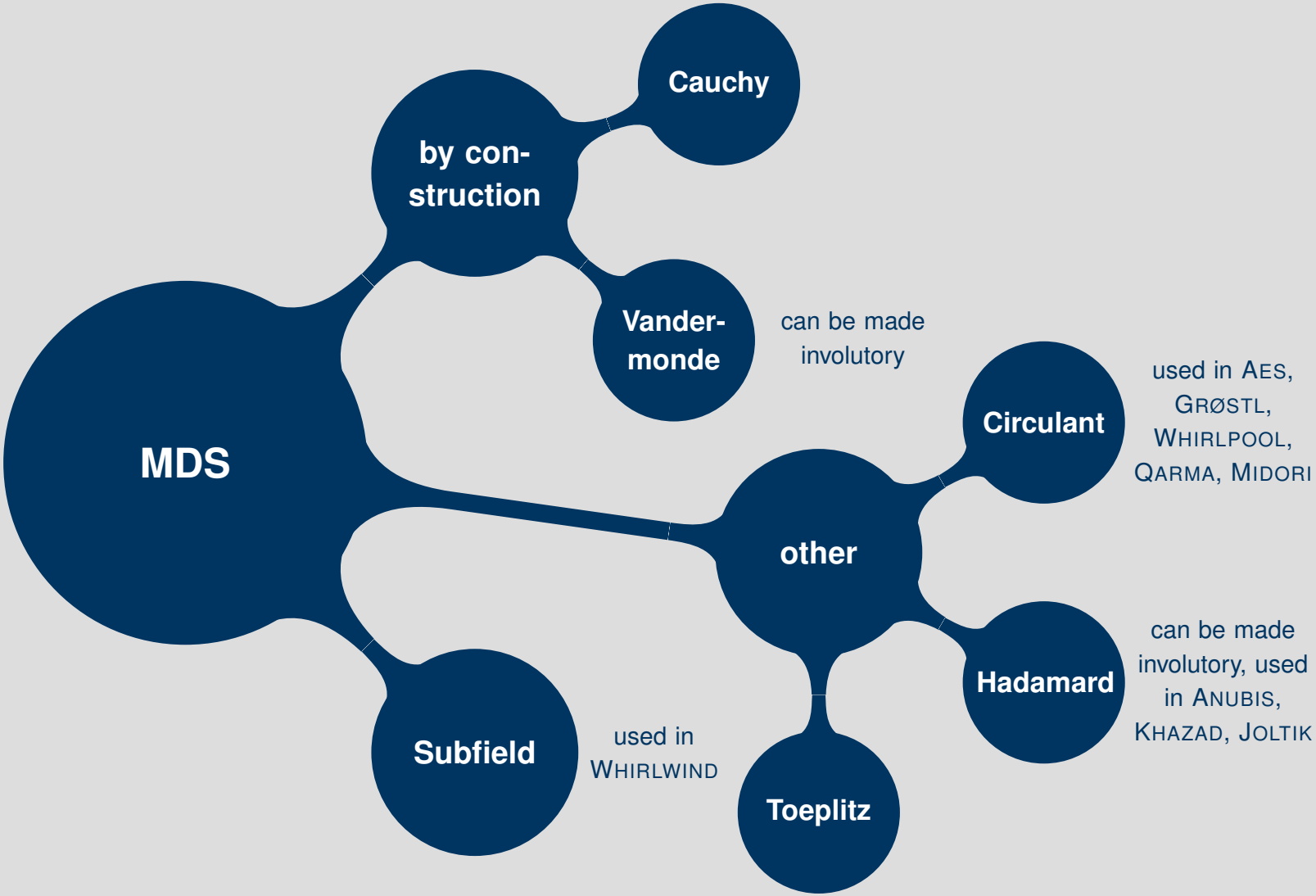
What is an MDS matrix?

Constructions



What is an MDS matrix?

Constructions



What is an MDS matrix?

Representations

What is an MDS matrix?

Representations

The General Linear Group

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