RUHR-UNIVERSITÄT BOCHUM

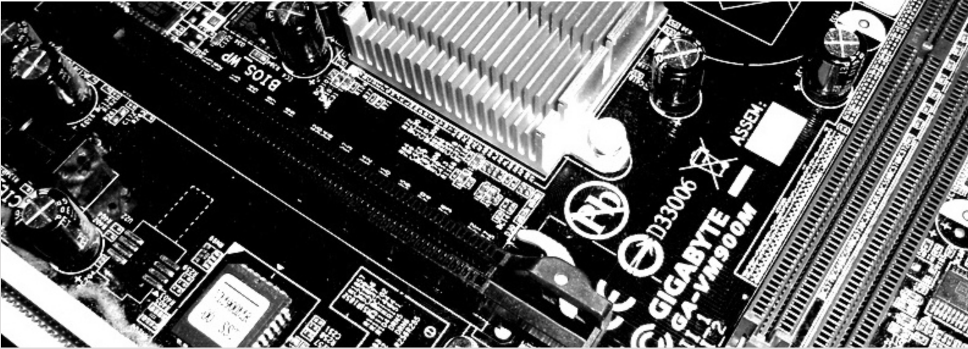
XOR Count

November 21st, 2017

FluxFingers

Workgroup Symmetric Cryptography
Ruhr University Bochum

Friedrich Wiemer



Overview

RUB

Joint Work – Its not me alone [Kra+17][1]

Thorsten Kranz, Gregor Leander, Ko Stoffelen, Friedrich Wiemer

RUHR UNIVERSITÄT BOCHUM RUB

Radboud University

Outline

[1] available on eprint: `https://eprint.iacr.org/2017/1151`

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

Some facts

- Lightweight Block Ciphers
- Efficient Linear Layers
- MDS matrices are “optimal” (regarding security)[2]

[2] 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)[2]
- What is the lightest implementable MDS matrix?
- What about additional features (Involutory)?

[2] 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)[2]
- What is the lightest implementable MDS matrix?
- What about additional features (Involutory)?

The XOR count

- Metric for needed hardware resources
- Smaller is better

[2] 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?

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

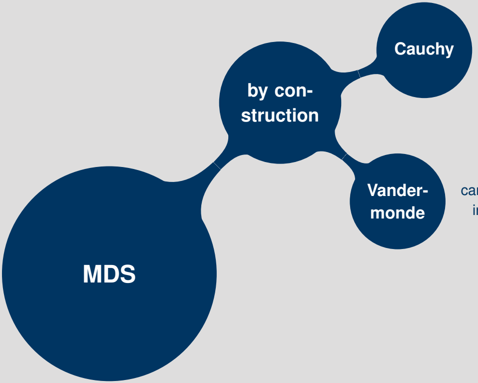
The AES MIXCOLUMN matrix is defined over $\mathbb{F}_{2^8} \cong \mathbb{F}[x]/\texttt{0x11b}$:

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

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

What is an MDS matrix?

Constructions

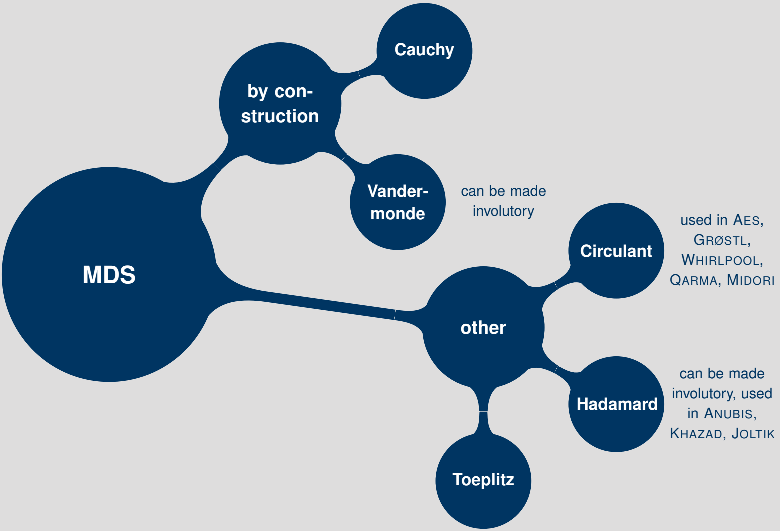


can be made involutory

What is an MDS matrix?

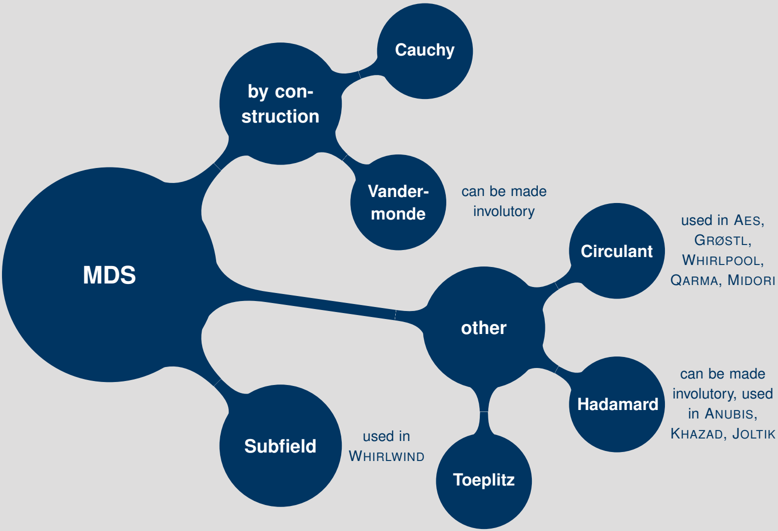
Constructions

RUB



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?

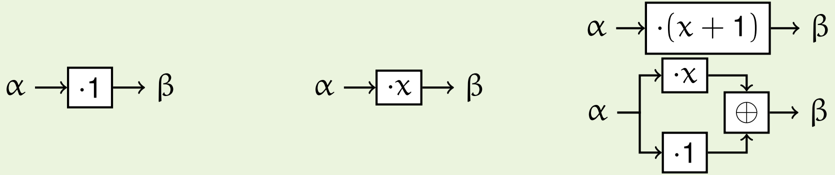
Representations

RUB

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



Field Multiplication in Hardware

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

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

OK, this one is easy ☺

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

Field Multiplication in Hardware

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

RUB

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

OK, this one is easy ☺

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

$$\alpha = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3$$

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

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

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

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

RUB

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 $(\mathbb{F}_2[x]/\text{0x11b})^{4\times4}$, we end up in $\left({\mathbb{F}_2}^{8\times8}\right)^{4\times4} \cong \mathbb{F}_2^{32\times32}$.

Counting XOR's

RUB

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 $(\mathbb{F}_2[x]/\text{0x11b})^{4\times4}$, we end up in $\left(\mathbb{F}_2{}^{8\times8}\right)^{4\times4} \cong \mathbb{F}_2^{32\times32}$.

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?

RUHR-UNIVERSITÄT BOCHUM

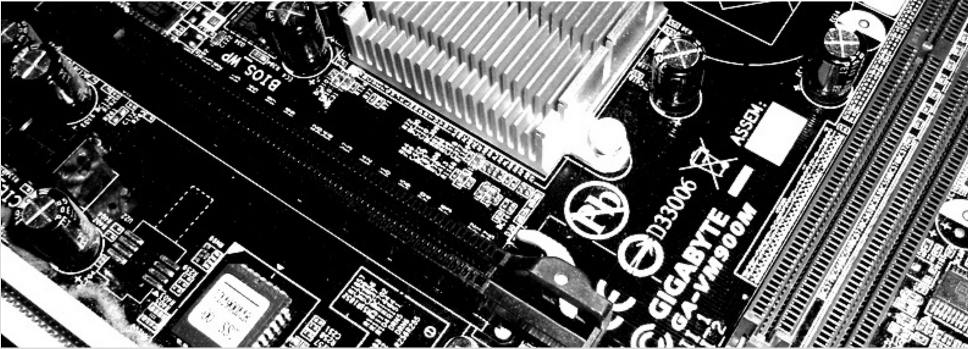
The Stupidity of recent XOR Count Papers

November 21st, 2017

FluxFingers

Workgroup Symmetric Cryptography
Ruhr University Bochum

Friedrich Wiemer



State of the Art

Before our Paper

- You saw how to count XORs
- This count is split in the “overhead” and the XORs needed for the field multiplication
- Thus for AES we get $56 + 8 \cdot 3 \cdot 4 = 56 + 96 = 152$
- Finding a good matrix reduces now to find the cheapest elements for field multiplication
- There is a lot of work followng this line [BKL16; JPS17; LS16; LW16; LW17; Sim+15; SS16a; SS16b; SS17; ZWS17]

State of the Art

Best known Results

RUB

4×4 matrices over $GL(8, \mathbb{F}_2)$		
Matrix	Naive	Literature
AES (Circulant)	152	**7+96**
[Sim+15] (Subfield)	136	40+96
[LS16] (Circulant)	128	32+96
[LW16]	106	10+96
[BKL16] (Circulant)	136	24+96
[SS16b] (Toeplitz)	123	27+96
[JPS17] (Subfield)	122	20+96

Related Work I

Optimized Arithmetic for Reed-Solomon Encoders

Christof Paar*
ECE Department
Worcester Polytechnic Institute
Worcester, MA 01609
email: christof@ece.wpi.edu

1997 IEEE International Symposium on Information Theory, June 29 -- July 4, 1997, Ulm, Germany (extended version)

Abstract

Multiplication with constant elements from Galois fields of characteristic two is the major arithmetic operation in Reed-Solomon encoders. This contribution describes two optimization algorithms which yield low complexity constant multipliers for Ga-

Related Work I

Optimized Arithmetic for Reed-Solomon Encoders

Christof Paar*
ECE Department
Worcester Polytechnic Institute
Worcester, MA 01609
email: `christof@ece.wpi.edu`

`1997 IEEE International Symposium on Information Theory, June 29 -- July 4, 1997, Ulm, Germany (extended version)`

Abstract

Multiplication with constant elements from Galois fields of characteristic two is the major arithmetic operation in Reed-Solomon encoders. This contribution describes two optimization algorithms which yield low complexity constant multipliers for Ga-

Related Work II

J. Cryptol. (2013) 26: 280–312
DOI: 10.1007/s00145-012-9124-7

Journal of
CRYPTOLOGY

Logic Minimization Techniques with Applications to Cryptology*

Joan Boyar†
Department of Mathematics and Computer Science, University of Southern Denmark, Odense, Denmark
joan@imada.sdu.dk

Philip Matthews‡
Aarhus University, Aarhus, Denmark

René Peralta
Information Technology Laboratory, NIST, Gaithersburg, MD, USA
rene.peralta@nist.gov

Communicated by Kaisa Nyberg

Received 8 February 2011
Online publication 3 May 2012

State of the Art

Best known Results (After our Paper)

4×4 matrices over $GL(8, \mathbb{F}_2)$

Matrix	Naive	Literature
AES (Circulant)	152	**7+96**
[Sim+15] (Subfield)	136	40+96
[LS16] (Circulant)	128	32+96
[LW16]	106	10+96
[BKL16] (Circulant)	136	24+96
[SS16b] (Toeplitz)	123	27+96
[JPS17] (Subfield)	122	20+96

RUB

State of the Art

Best known Results (After our Paper)

4×4 matrices over $GL(8, \mathbb{F}_2)$					
			Our Results [Kra+17]		
Matrix	Naive	Literature	PAAR1	PAAR2	BP
AES (Circulant)	152	**7+96**	108	108	97
[Sim+15] (Subfield)	136	40+96	100	98	100
[LS16] (Circulant)	128	32+96	116	116	112
[LW16]	106	10+96	102	102	102
[BKL16] (Circulant)	136	24+96	116	112	110
[SS16b] (Toeplitz)	123	27+96	110	108	107
[JPS17] (Subfield)	122	20+96	96	95	**86**

State of the Art

Finding better matrices?

RUB

Type	Previously Best Known		XOR count
$\mathrm{GL}(4, \mathbb{F}_2)^{4\times4}$	58	[JPS17; SS16b]	36
$\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$	106	[LW16]	72
$(\mathbb{F}_2[x]/\texttt{0x13})^{8\times8}$	392	[Sim+15]	196
$\mathrm{GL}(8, \mathbb{F}_2)^{8\times8}$	640	[LS16]	392
$(\mathbb{F}_2[x]/\texttt{0x13})^{4\times4\star}$	63	[JPS17]	42
$\mathrm{GL}(8, \mathbb{F}_2)^{4\times4}$	126	[JPS17]	84
$(\mathbb{F}_2[x]/\texttt{0x13})^{8\times8}$	424	[Sim+15]	212
$\mathrm{GL}(8, \mathbb{F}_2)^{8\times8}$	663	[JPS17]	424

Future Work; Questions?

Thank you for your attention!

Do your work!

Apply global optimization techniques that are known for years!

(But thanks for the easy paper ☺)

Mainboard & Questionmark Images: flickr

References I

[BKL16] C. Beierle, T. Kranz, and G. Leander. "Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices". In: *CRYPTO 2016, Part I*. Ed. by M. Robshaw and J. Katz. Vol. 9814. LNCS. Springer, Heidelberg, Aug. 2016, pp. 625–653. DOI: 10.1007/978-3-662-53018-4_23.

[JPS17] J. Jean, T. Peyrin, and S. M. Sim. *Optimizing Implementations of Lightweight Building Blocks*. Cryptology ePrint Archive, Report 2017/101. http://eprint.iacr.org/2017/101. 2017.

[Kra+17] T. Kranz, G. Leander, K. Stoffelen, and F. Wiemer. "Shorter Linear Straight-Line Programs for MDS Matrices". In: *IACR Trans. Symm. Cryptol.* 2017.4 (2017). to appear. ISSN: 2519-173X.

[LS16] M. Liu and S. M. Sim. "Lightweight MDS Generalized Circulant Matrices". In: *FSE 2016*. Ed. by T. Peyrin. Vol. 9783. LNCS. Springer, Heidelberg, Mar. 2016, pp. 101–120. DOI: 10.1007/978-3-662-52993-5_6.

[LW16] Y. Li and M. Wang. "On the Construction of Lightweight Circulant Involutory MDS Matrices". In: *FSE 2016*. Ed. by T. Peyrin. Vol. 9783. LNCS. Springer, Heidelberg, Mar. 2016, pp. 121–139. DOI: 10.1007/978-3-662-52993-5_7.

References II

[LW17] C. Li and Q. Wang. “Design of Lightweight Linear Diffusion Layers from Near-MDS Matrices”. In: *IACR Trans. Symm. Cryptol.* 2017.1 (2017), pp. 129–155. ISSN: 2519-173X. DOI: 10.13154/tosc.v2017.i1.129-155.

[Sim+15] S. M. Sim, K. Khoo, F. E. Oggier, and T. Peyrin. “Lightweight MDS Involution Matrices”. In: *FSE 2015*. Ed. by G. Leander. Vol. 9054. LNCS. Springer, Heidelberg, Mar. 2015, pp. 471–493. DOI: 10.1007/978-3-662-48116-5_23.

[SS16a] S. Sarkar and S. M. Sim. “A Deeper Understanding of the XOR Count Distribution in the Context of Lightweight Cryptography”. In: *AFRICACRYPT 2016*. Ed. by D. Pointcheval, A. Nitaj, and T. Rachidi. Vol. 9646. LNCS. Springer International Publishing, 2016, pp. 167–182.

[SS16b] S. Sarkar and H. Syed. “Lightweight Diffusion Layer: Importance of Toeplitz Matrices”. In: *IACR Trans. Symm. Cryptol.* 2016.1 (2016). http://tosc.iacr.org/index.php/ToSC/article/view/537, pp. 95–113. ISSN: 2519-173X. DOI: 10.13154/tosc.v2016.i1.95-113.

[SS17] S. Sarkar and H. Syed. “Analysis of Toeplitz MDS Matrices”. In: *ACISP 17, Part II*. Ed. by J. Pieprzyk and S. Suriadi. Vol. 10343. LNCS. Springer, Heidelberg, July 2017, pp. 3–18.

References III

[ZWS17] L. Zhou, L. Wang, and Y. Sun. *On the Construction of Lightweight Orthogonal MDS Matrices*. Cryptology ePrint Archive, Report 2017/371. `http://eprint.iacr.org/2017/371`. 2017.