Lightweight MDS Involution Matrices

Siang Meng Sim[1] Khoongming Khoo[2]
Frédérique Oggier[1] Thomas Peyrin[1]

1.Nanyang Technological University, Singapore

2.DSO National Laboratories, Singapore

10 March 2015

Table of Contents

1. Introduction
2. Analyzing XOR Count
3. Equivalence Classes of Hadamard-based Matrices
   - Equivalence Classes of Hadamard Matrices
   - Equivalence Classes of Involutory Hadamard-Cauchy Matrices
4. Comparisons with Existing MDS Matrices

Table of Contents

1 Introduction

2 Analyzing XOR Count

3 Equivalence Classes of Hadamard-based Matrices
- Equivalence Classes of Hadamard Matrices
- Equivalence Classes of Involutory Hadamard-Cauchy Matrices

4 Comparisons with Existing MDS Matrices

Diffusion Matrices

The diffusion layer of a cipher provides the diffusion property - spread the internal dependencies as much as possible.

The diffusion power of a diffusion matrix can be quantified by the branch number, $\mathcal{B}$.

Branch number

For any nonzero input, the sum of nonzero components of the input and output is at least $\mathcal{B}$.

Maximal Distance Separable (MDS) Matrices

For a $k \times k$ matrix, the largest possible branch number is $k + 1$. Matrices that attain this bound are known as MDS matrices.

The diffusion matrix in AES over $\mathrm{GF}(2^8)$.

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

It has a branch number of 5 and it is MDS.

Involution Matrices

Involution (self-inverse) matrices are very interesting as the same matrix can be used for encryption and decryption.

For hardware implementation, we use XOR count to evaluate the lightweightness of a given matrix.

Diffusion matrix	**Encryption cost** (XOR count)	**Decryption cost** (XOR count)	**Total cost** (XOR count)
AES diffusion matrices	38	110	**148**
Involution matrix	40	-	**40**

In our paper, we focus on MDS involution matrices.

Table of Contents

1 Introduction

2 Analyzing XOR Count

3 Equivalence Classes of Hadamard-based Matrices
- Equivalence Classes of Hadamard Matrices
- Equivalence Classes of Involutory Hadamard-Cauchy Matrices

4 Comparisons with Existing MDS Matrices

Notation

Notation

$\mathrm{GF}(2^r)/p(x)$ is the finite field defined by irreducible polynomial $p(x)$ that is expressed as hexadecimal.

Evaluate the weight of a matrix

The number of XOR needed for the multiplication of its entries.

XOR Count for Hardware Implementation

We use the following formula [Khoo *et al.* - CHES 2014] to calculate the number of XORs required to implement an entire row of a matrix:

$$\text{XOR count for one row of } M = \sum_{i=1}^{k} \gamma_i + (n-1) \cdot r,$$

where γ_i is the XOR count of the i-th entry in the row, n being the number of nonzero elements in the row and r the dimension of the finite field.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2x_0 + 3x_1 + x_2 + x_3 \\ * \\ * \\ * \end{pmatrix}$$

XOR Count (Example)

Let $\alpha = 3$ over $\mathrm{GF}(2^3)$ defined by $x^3 + x + 1$.
Let (b_2, b_1, b_0) be the binary representation of an arbitrary element β in the field.

$$\begin{aligned}(0,1,1) \cdot (b_2, b_1, b_0) =&(b_1, b_0 \oplus b_2, b_2) \oplus (b_2, b_1, b_0) \\ =&(b_1 \oplus b_2, b_0 \oplus b_1 \oplus b_2, b_0 \oplus b_2)\end{aligned}$$

The XOR count of 3 over $\mathrm{GF}(2^3)/0xb$ is 4.

On the other hand, for $\mathrm{GF}(2^3)$ defined by $x^3 + x^2 + 1$.

$$\begin{aligned}(0,1,1) \cdot (b_2, b_1, b_0) =&(b_1 \oplus b_2, b_0, b_2) \oplus (b_2, b_1, b_0) \\ =&(b_1, b_0 \oplus b_1, b_0 \oplus b_2)\end{aligned}$$

The XOR count of 3 over $\mathrm{GF}(2^3)/0xd$ is 2.

Choice of Finite Fields

Question:

which irreducible polynomial to use to define the finite field?

The folklore was to always choose low hamming weight polynomial.

AES matrix is over $\mathrm{GF}(2^8)/0\text{x}11b$, with hamming weight 5.

But there are many more low hamming weight polynomials: $0\text{x}12b, 0\text{x}163, 0\text{x}165, 0\text{x}1c3$, etc.

Our Recommendation

Question:

which irreducible polynomial to use to define the finite field?

Answer:

finite fields with high standard deviation of XOR count distribution

- in general, the order of the finite field is much larger than the order of the matrix
- high standard deviation (s.d.) implies that more elements with relatively lower/higher XOR count
- there is a high chance that an MDS matrix contains elements with lower XOR count

XOR Count Distributions

We have found the lightest MDS matrices over $\mathrm{GF}(2^8)$ from 0x165 and 0x1c3.

x	$\mathrm{GF}(2^8)$				
	0x11b	0x12b	0x163	0x165	0x1c3
mean	24.03	24.03	24.03	24.03	24.03
s.d.	6.7574	6.1752	6.4144	6.8679	7.4634

The best choice of polynomial might not necessarily be among the low hamming weight ones, but those with high standard deviation.

Table of Contents

1 Introduction

2 Analyzing XOR Count

3 Equivalence Classes of Hadamard-based Matrices
- Equivalence Classes of Hadamard Matrices
- Equivalence Classes of Involutory Hadamard-Cauchy Matrices

4 Comparisons with Existing MDS Matrices

Hadamard Matrices

A finite field Hadamard (or simply called Hadamard) matrix H is a square matrix of order 2^s, that can be represented by two other submatrices H_1 and H_2 which are also Hadamard matrices:

$$H = \begin{pmatrix} H_1 & H_2 \\ H_2 & H_1 \end{pmatrix}.$$

Notation

A Hadamard matrix can be denoted by its first row, $Had(h_0, h_1, h_2, ..., h_{2^s-1})$.

Properties of Hadamard Matrices

Hardware implementation

Every row is a permutation of its first row, round-based implementation can be used.

Product of Hadamard matrix

$H \times H = cI$, where I is identity matrix and $c = (h_0 + h_1 + ... + h_{2^s-1})^2$.
It is an involution matrix if the sum of the first row is 1.

Branch number of Hadamard matrix

Different permutation of the entries may have different branch number.

Table of Contents

1 Introduction

2 Analyzing XOR Count

3 Equivalence Classes of Hadamard-based Matrices
- Equivalence Classes of Hadamard Matrices
- Equivalence Classes of Involutory Hadamard-Cauchy Matrices

4 Comparisons with Existing MDS Matrices

Motivation

Finding lightweight MDS involution matrices:

choose a set of 2^s elements that

- has the lowest possible total XOR count, and
- sum to 1

as the first row of a Hadamard matrix.

For each permutation of the set, we check if it is MDS.

Problem:

there are $2^s!$ ways to permute, which can quickly be intractable.

Equivalence Classes

We group the Hadamard matrices into equivalence classes to significantly reduce the search space.

Equivalence Classes of Hadamard Matrices

Hadamard matrices within an equivalence class have the same set of entries (up to permutation) and the same branch number.

It is sufficient to check one representative from each equivalence class.

Number of Equivalence Classes

We provide

- a formula to count the number of equivalence classes, and
- an algorithm to generate one representative from each equivalence classes.

Order of the matrix	Total no. of permutations	Total no. of Equivalence Classes
4	24	1
8	$40,320$	30
16	$2^{44.3}$	2^{26}
32	$2^{117.7}$	$2^{89.4}$

Using the equivalence classes, the search space decreases exponentially.

Exhaustive Search Algorithm

1. pick a set of 2^s elements that is lightweight and sum to 1
2. `FOR` each representative, check MDS:
   - `YES` - terminate the algorithm prematurely and output the MDS matrix
   - `NO` - check the next representative
3. output that there is no MDS Hadamard matrix for the given set of elements

Table of Contents

1. Introduction
2. Analyzing XOR Count
3. Equivalence Classes of Hadamard-based Matrices
   - Equivalence Classes of Hadamard Matrices
   - Equivalence Classes of Involutory Hadamard-Cauchy Matrices
4. Comparisons with Existing MDS Matrices

Motivation

The computational cost for testing MDS becomes too huge when the order is larger than 8.

Hadamard-Cauchy Matrices

The construction of Hadamard-Cauchy matrices is proposed by Gupta *et al.* in AFRICACRYPT 2013 that combines both the characteristics of Hadamard and Cauchy matrices.

- Hadamard - It is involution when the sum of first row is 1
- Cauchy - It is MDS based on the construction.

Motivation

Disadvantage:

there is little control over the entries of the matrix.

Direct way:

generate all possible involutory Hadamard-Cauchy matrices and pick the lightest.

Problem:

for matrix of order 32 over $\mathrm{GF}(2^8)$, there are about $2^{47.6}$ different Hadamard-Cauchy matrices to compare, which is too time consuming on a small cluster.

Equivalence Classes

We group the Hadamard-Cauchy matrices into equivalence classes to significantly reduce the search space.

Equivalence Classes of Involutory Hadamard-Cauchy Matrices

Involutory Hadamard-Cauchy matrices within an equivalence class have the same set of entries (up to permutation) and the same XOR count.

It is sufficient to store one representative from each equivalence class and pick the lightest.

Number of Equivalence Classes

We provide

- a formula to count the number of equivalence classes, and
- an algorithm to find the lightest involutory Hadamard-Cauchy matrix.

Order of the matrix over $\mathrm{GF}(2^8)$	Total no. of H-C Matrices	Total no. of Equivalence Classes
16	$2^{39.9}$	11811
32	$2^{47.6}$	2667

When the dimension of the order is more than half of the dimension of the finite field, the number of equivalence classes decreases.

Exhaustive Search Algorithm

1. compute the number of equivalence classes, EC
2. `WHILE` number of matrices stored $< EC$
   1. generate an involutory Hadamard-Cauchy matrix
   2. check if it belongs to some stored equivalence class:
      - `YES` - goto step 2.1
      - `NO` - store that matrix
3. output the lightest involutory Hadamard-Cauchy matrix

Table of Contents

1 Introduction

2 Analyzing XOR Count

3 Equivalence Classes of Hadamard-based Matrices
- Equivalence Classes of Hadamard Matrices
- Equivalence Classes of Involutory Hadamard-Cauchy Matrices

4 Comparisons with Existing MDS Matrices

Comparison of MDS Involution Matrices

MDS INVOLUTION MATRICES

matrix type	finite field	coefficients of the first row	XOR count	reference
4×4 **matrix**				
Hadamard	$GF(2^8)$/0x165	(0x01, 0x02, 0xb0, 0xb2)	$16 + 3 \times 8 = \mathbf{40}$	Our paper
Hadamard	$GF(2^8)$/0x11d	(0x01, 0x02, 0x04, 0x06)	$22 + 3 \times 8 = \mathbf{46}$	ANUBIS
8×8 **matrix**				
Hadamard	$GF(2^8)$/0x1c3	(0x01, 0x02, 0x03, 0x91, 0x04, 0x70, 0x05, 0xe1)	$46 + 7 \times 8 = \mathbf{102}$	Our paper
Hadamard	$GF(2^8)$/0x11d	(0x01, 0x03, 0x04, 0x05, 0x06, 0x08, 0x0b, 0x07)	$98 + 7 \times 8 = \mathbf{154}$	KHAZAD
16×16 **matrix**				
Hadamard-Cauchy	$GF(2^8)$/0x1c3	(0x08, 0x16, 0x8a, 0x01, 0x70, 0x8d, 0x24, 0x76, 0xa8, 0x91, 0xad, 0x48, 0x05, 0xb5, 0xaf, 0xf8)	$258 + 15 \times 8 = \mathbf{378}$	Our paper
Hadamard-Cauchy	$GF(2^8)$/0x11b	(0x01, 0x03, 0x08, 0xb2, 0x0d, 0x60, 0xe8, 0x1c, 0x0f, 0x2c, 0xa2, 0x8b, 0xc9, 0x7a, 0xac, 0x35)	$338 + 15 \times 8 = \mathbf{458}$	Gupta et al.
32×32 **matrix**				
Hadamard-Cauchy	$GF(2^8)$/0x165	(0xd2, 0x06, 0x05, 0x4d, 0x21, 0xf8, 0x11, 0x62, 0x08, 0xd8, 0xe9, 0x28, 0x4b, 0x96, 0x10, 0x2c, 0xa1, 0x49, 0x4c, 0xd1, 0x59, 0xb2, 0x13, 0xa4, 0x03, 0xc3, 0x42, 0x79, 0xa0, 0x6f, 0xab, 0x41)	$610 + 31 \times 8 = \mathbf{858}$	Our paper
Hadamard-Cauchy	$GF(2^8)$/0x11b	(0x01, 0x02, 0x04, 0x69, 0x07, 0xec, 0xcc, 0x72, 0x0b, 0x54, 0x29, 0xbe, 0x74, 0xf9, 0xc4, 0x87, 0x0e, 0x47, 0xc2, 0xc3, 0x39, 0x8e, 0x1c, 0x85, 0x58, 0x26, 0x1e, 0xaf, 0x68, 0xb6, 0x59, 0x1f)	$675 + 31 \times 8 = \mathbf{923}$	Gupta et al.

Comparison of MDS Non-Involution Matrices

Our methods can be relaxed and applied to search for lightweight MDS non-involution matrices as well.

MDS NON-INVOLUTION MATRICES

matrix type	finite field	coefficients of the first row	XOR count	reference
4×4 **matrix**				
Hadamard	$\mathrm{GF}(2^8)/\mathrm{0x1c3}$	$(\mathrm{0x01}, \mathrm{0x02}, \mathrm{0x04}, \mathrm{0x91})$	$13 + 3 \times 8 = \mathbf{37}$	Our paper
Circulant	$\mathrm{GF}(2^8)/\mathrm{0x11b}$	$(\mathrm{0x02}, \mathrm{0x03}, \mathrm{0x01}, \mathrm{0x01})$	$14 + 3 \times 8 = \mathbf{38}$	AES
8×8 **matrix**				
Hadamard	$\mathrm{GF}(2^8)/\mathrm{0x1c3}$	$(\mathrm{0x01}, \mathrm{0x02}, \mathrm{0x03}, \mathrm{0x08}, \mathrm{0x04}, \mathrm{0x91}, \mathrm{0xe1}, \mathrm{0xa9})$	$40 + 7 \times 8 = \mathbf{96}$	Our paper
Circulant	$\mathrm{GF}(2^8)/\mathrm{0x11d}$	$(\mathrm{0x01}, \mathrm{0x01}, \mathrm{0x04}, \mathrm{0x01}, \mathrm{0x08}, \mathrm{0x05}, \mathrm{0x02}, \mathrm{0x09})$	$49 + 7 \times 8 = \mathbf{105}$	WHIRLPOOL
Circulant	$\mathrm{GF}(2^8)/\mathrm{0x11d}$	WHIRLPOOL-like matrices	between **105** to **117**	

Most existing Hadamard-based matrices are designed to be involution (and are a bit more costly), thus we only compare here with circulant matrices.

Our Hadamard-based Matrices

4×4 MDS involutory Hadamard matrix over $\mathrm{GF}(2^8)$/0x165

$$\begin{bmatrix} 1 & 2 & 176 & 178 \\ 2 & 1 & 178 & 176 \\ 176 & 178 & 1 & 2 \\ 178 & 176 & 2 & 1 \end{bmatrix}$$

Our Hadamard-based Matrices

16×16 involutory Hadamard-Cauchy matrix over $\mathrm{GF}(2^8)/0\mathrm{x}1c3$

8	22	138	1	112	141	36	118	168	145	173	72	5	181	175	248
22	8	1	138	141	112	118	36	145	168	72	173	181	5	248	175
138	1	8	22	36	118	112	141	173	72	168	145	175	248	5	181
1	138	22	8	118	36	141	112	72	173	145	168	248	175	181	5
112	141	36	118	8	22	138	1	5	181	175	248	168	145	173	72
141	112	118	36	22	8	1	138	181	5	248	175	145	168	72	173
36	118	112	141	138	1	8	22	175	248	5	181	173	72	168	145
118	36	141	112	1	138	22	8	248	175	181	5	72	173	145	168
168	145	173	72	5	181	175	248	8	22	138	1	112	141	36	118
145	168	72	173	181	5	248	175	22	8	1	138	141	112	118	36
173	72	168	145	175	248	5	181	138	1	8	22	36	118	112	141
72	173	145	168	248	175	181	5	1	138	22	8	118	36	141	112
5	181	175	248	168	145	173	72	112	141	36	118	8	22	138	1
181	5	248	175	145	168	72	173	141	112	118	36	22	8	1	138
175	248	5	181	173	72	168	145	36	118	112	141	138	1	8	22
248	175	181	5	72	173	145	168	118	36	141	112	1	138	22	8

Application

One of the CAESAR candidates - `JOLTIK`, designed by Jean *et al.*, that is lightweight and hardware-oriented uses our lightweight MDS involution matrix of order 4 over $\mathrm{GF}(2^4)/$0x13.

$$\begin{bmatrix} 1 & 4 & 9 & 13 \\ 4 & 1 & 13 & 9 \\ 9 & 13 & 1 & 4 \\ 13 & 9 & 4 & 1 \end{bmatrix}$$

Summary

- Recommend choosing finite fields with high standard deviation regarding XOR counts to find lightweight MDS matrices.
- Propose the concept of equivalence classes of Hadamard-based matrices to significantly reduce the search space.
- Present the lightest possible (involutory) Hadamard matrices of order 4 and 8 over $\mathrm{GF}(2^4)$ and $\mathrm{GF}(2^8)$, the (involutory) Hadamard-Cauchy matrices of order 16 and 32 over $\mathrm{GF}(2^8)$.

Conclusion

Involution matrices should be used as they:

- do not cost much more than non-involution matrices, and
- can save more than half of the space when both encryption and decryption are required.

Diffusion matrix	Encryption cost	Decryption cost	Total cost
AES diffusion matrices	38	110	**148**
Our involution matrix	40	-	**40**

Thank you. :)