On Efficient Constructions of Lightweight MDS Matrices

Lijing Zhou, Licheng Wang and Yiru Sun

State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications

FSE 2018, Bruges, Belgium
March , 2018

Outline

1. **Background and Motivations**
2. **Efficiently Construct Lightweight MDS Matrices**
3. **Efficiently Construct Involutory Hadamad MDS Matrices**

Outline

1. **Background and Motivations**
2. **Efficiently Construct Lightweight MDS Matrices**
3. **Efficiently Construct Involutory Hadamad MDS Matrices**

Linear diffusion layer

A linear diffusion layer can be represented by a matrix and provides external dependency.

Let L be a linear diffusion layer which is a matrix of order n. L's performance is measured by the branch number:

- $B(L) = \min\{w(X) + w(LX) \mid X \in (F_2^m)^n, X \neq 0\}$
- $B(L) \leq n+1$

MDS Matrix

L is an MDS matrix of order n if and only if $B(L)=n+1$.

Lightweight MDS Matrix

Blaum, Roth, IEEE TIT 1999

L is MDS if and only if all square sub-matrices of L are of full rank.

Lightweight MDS Matrix

An MDS matrix of order n can be represented by the following matrix:

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix}$$

where $L_{i,j}$ are non-singular binary matrices of order m.

For convenience, L is called the structure-matrix (or structure), and $L_{i,j}$ is called the entry-matrix (or entry).

XOR Count and Full Rank

XOR count

Lightweight means the implementation requires fewer XORs.

- XOR count of $L_{i,j}$ is described by $\#(L_{i,j})=w(L_{i,j})-m$.

- XOR count of L is described by $\#(L)$, which is the sum of all XOR counts of $L_{i,j}$.

Full rank

Let A, B and C be binary matrices of order 4.

That $\begin{pmatrix} A & B & C \\ C & A & B \\ B & C & A \end{pmatrix}$ is of full rank means that its rank is 12.

Motivations

1. Efficiency

$$\begin{pmatrix} I & I & A & B \\ B & I & I & A \\ A & B & I & I \\ I & A & B & I \end{pmatrix} \quad \begin{pmatrix} I & A & B & C \\ A & I & C & B \\ B & C & I & A \\ C & B & A & I \end{pmatrix} \quad \begin{pmatrix} A & I & I & I \\ I & I & B & A \\ I & A & I & B \\ I & B & A & I \end{pmatrix} \quad \begin{pmatrix} I & I & I & X \\ I & A & B & I \\ I & B & A & A \\ X & I & A & I \end{pmatrix}$$

Circulant matrix — Hadamard matrix — Optimal matrix (special) — Other matrix

$$\underset{S_1}{\begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ I & F & G & I \end{pmatrix}} \quad \underset{S_2}{\begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ F & G & H & I \end{pmatrix}} \quad \underset{S_3}{\begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ F & G & I & H \end{pmatrix}} \quad \underset{S_4}{\begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ I & F & G & H \end{pmatrix}} \quad \underset{S_5}{\begin{pmatrix} I & I & A & B \\ C & I & I & D \\ E & F & I & I \\ I & G & H & I \end{pmatrix}}$$

Motivations

2. Entry

- Matrix representation of finite field F_{2^m}
- The set of all non-singular binary matrices $GL(m, F_2)$

Outline

1. **Background and Motivations**
2. **Efficiently Construct Lightweight MDS Matrices**
3. **Efficiently Construct Involutory Hadamad MDS Matrices**

Structure-matrices

$$\underset{S_1}{\begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ I & F & G & I \end{pmatrix}} \quad \underset{S_2}{\begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ F & G & H & I \end{pmatrix}} \quad \underset{S_3}{\begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ F & G & I & H \end{pmatrix}} \quad \underset{S_4}{\begin{pmatrix} A & I & I & I \\ I & I & B & C \\ I & D & I & E \\ I & F & G & H \end{pmatrix}} \quad \underset{S_5}{\begin{pmatrix} I & I & A & B \\ C & I & I & D \\ E & F & I & I \\ I & G & H & I \end{pmatrix}}$$

Method to select the structures: no sub-matrix $\begin{pmatrix} I & I \\ I & I \end{pmatrix}$

Entry From Matrix Polynomial Residue Ring

Let T be a non-singular binary matrix.

$f(x)$ is the minimal polynomial of T. It satisfies $f(T)=0$.

$F_2(T)$ is isomorphic to $F_2[x]/(f(x))$.

$F_2(T)$ is the matrix polynomial residue ring generated by T.

$$\begin{pmatrix} T & I & I & I \\ I & I & a(T) & T \\ I & T & I & b(T) \\ I & c(T) & d(T) & I \end{pmatrix}$$

1 XOR

Identify Full Rank

$$\begin{pmatrix} T & I & I \\ I & I & T \\ I & T^2+I & I \end{pmatrix} \rightarrow \begin{pmatrix} x & 1 & 1 \\ 1 & 1 & x \\ 1 & x^2+1 & 1 \end{pmatrix} \rightarrow \begin{vmatrix} x & 1 & 1 \\ 1 & 1 & x \\ 1 & x^2+1 & 1 \end{vmatrix} = x^4+1$$

Sub-matrix Sub-matrix Sub-determinant

$$T^4+I$$

$$\begin{pmatrix} T & I & I \\ I & I & T \\ I & T^2+I & I \end{pmatrix}$$ is of full rank if and only if T^4+I non-singular.

Conditions of *T*

Let *T* be a binary matrix of order *m*. *T* satisfies the following conditions:

1. $\#(T)=1$

2. *T* is non-singular

3. $T+I$ is non-singular

Conditions of T

Why is $T+I$ non-singular?

Conditions of T

$$
\begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ I & & & I \end{pmatrix}
\quad
\begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ & & & I \end{pmatrix}
\quad
\begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ & & I & \end{pmatrix}
\quad
\begin{pmatrix} & I & I & I \\ I & I & & \\ I & & I & \\ I & & & \end{pmatrix}
\quad
\begin{pmatrix} I & I & & \\ & I & I & \\ & & I & I \\ I & & & I \end{pmatrix}
$$

$$
S_1 \qquad\qquad S_2 \qquad\qquad S_3 \qquad\qquad S_4 \qquad\qquad S_5
$$

If there are at least two T in one of the above structures, then there must exist a sub-matrix as the following matrix:

$$
\begin{pmatrix} I & I \\ I & T \end{pmatrix}
$$

$\begin{pmatrix} I & I \\ I & T \end{pmatrix}$ is of full rank if and only if $T+I$ is non-singular.

Analyzing $F_2(T)$

For instance, T's order is 8. By searching T, we get:

1. The number of T is 28224.
2. The minimal polynomial of T only has 7 choices.
3. In any $F_2[T]$, there are at most 4 elements with no more than 3 XORs.

Algorithm 1

Step 1: Select T satisfying #(T)=1, T and $T+I$ are non-singular, and find its minimal polynomial $f(x)$. Then, find $b_1(x)$, $b_2(x)$, $b_3(x)$, $b_4(x)$ satisfying $\# b(T) \leq 3$ XORs.

Step 2: Construct candidates over $\{b_1(x), b_2(x), b_3(x), b_4(x)\}$.

$$\rightarrow \begin{pmatrix} x & 1 & 1 & 1 \\ 1 & 1 & x^2+1 & x \\ 1 & x & 1 & x^2+1 \\ 1 & x^2+1 & x & 1 \end{pmatrix}$$

Step 3: If the matrix is MDS, then output the right matrix and its XORs.

$$\rightarrow \begin{pmatrix} T & I & I & I \\ I & I & T^2+I & T \\ I & T & I & T^2+I \\ I & T^2+I & T & I \end{pmatrix}$$

Comparisons with LB16

Entries are matrices of order 4.

Matrix type	Sum of XORs	Number of results	Running time	Ref.
Special structure-matrix	10	845	1 week	LB16
S_1	10	288	00:01:42	Ours

LB16: Intel Core i7-4790 16 G 3.6 GHz

Our platform: C-free Intel Core i5-5300U 4G 2.3GHz

Comparisons with LW16 (FSE2016)

Entries are matrices of order 8.

Matrix type	Sum of XORs	Number of results	Running time	Ref.
$Circulant(I, I, A, B)$	12	80640	3 days	LW16
$Circulant(I, I, A, B)$	12	80640	00:01:27	Ours
$Had(I, A, A^T, B)$	20	622	4 weeks	LW16
$Had(I, A, B, C)$	20	241920	00:07:00	Ours

LW16 (FSE2016): Magma v2.20-3 Intel Core i5

Our platform: C-free Intel Core i5-5300U 4G 2.30GHz

Results

Matrix type	Entries	Sum of XORs	Number of results	Running time
$Circ(I, I, A, B)$	$F_2[T_{4\times4}]$	12	96	00:00:01
$Hada(I, A, B, C)$	$F_2[T_{4\times4}]$	20	288	00:00:04
Optimal (special)	$F_2[T_{4\times4}]$	13	48	00:00:01
S_1	$F_2[T_{4\times4}]$	10	288	00:01:42
S_3	$F_2[T_{4\times4}]$	10	48	00:05:05
$Circ(I, I, A, B)$	$F_2[T_{8\times8}]$	12	80640	00:01:27
$Hada(I, A, B, C)$	$F_2[T_{8\times8}]$	20	241920	00:07:00
Optimal (special)	$F_2[T_{8\times8}]$	10	40320	00:01:16
S_1	$F_2[T_{8\times8}]$	10	1128960	14:00:00
$Circ(I, I, A, B)$	$F_2[T_{16\times16}]$	12	1	00:00:30
Optimal (special)	$F_2[T_{16\times16}]$	10	1	00:00:30

Our platform: C-free Intel Core i5-5300U 4G 2.30GHz

Outline

1. **Background and Motivations**
2. **Efficiently Construct Lightweight MDS Matrices**
3. **Efficiently Construct Involutory Hadamad MDS Matrices**

Involutory matrix

L is an involutory matrix if and only if $L^2 = I$

$$\begin{pmatrix} I & A & B & C \\ A & I & C & B \\ B & C & I & A \\ C & B & A & I \end{pmatrix}^2 = \begin{pmatrix} I & & & \\ & I & & \\ & & I & \\ & & & I \end{pmatrix}$$

Involutory Hadamard MDS matrix

Hada(I, A, B, C) denotes the following Hadamard matrix.

$$\begin{pmatrix} I & A & B & C \\ A & I & C & B \\ B & C & I & A \\ C & B & A & I \end{pmatrix}$$

Theorem 1: $T \in GL(m,\mathrm{F}_2)$, $f(x)$ is the minimal polynomial of T. $a(x)$, $b(x)$, $c(x)$ $\in F_2[x]/(f(x))$. Then *Hada*(1, $a(x)$, $b(x)$, $c(x)$) is involutory if and only if

$$a(x)^2 \equiv (\ b(x) + c(x)\ )^2 \mod f(x)$$

Special case: *Hada*(1, x, $b(x)$, $c(x)$) is involutory if and only if

$$x^2 \equiv (\ b(x) + c(x)\ )^2 \mod f(x)$$

Involutory Hadamard MDS matrix

Special case: $Hada(1, x, b(x), c(x))$ is involutory if and only if

$$x^2 \equiv (b(x) + c(x))^2 \mod f(x)$$

For instance, $g_0(x)$ satisfies $x^2 \equiv (g_0(x))^2 \mod f_1(x)$. Let

$$c(x)=b(x)+ g_0(x).$$

It is equivalent to $b(x) + c(x) = g_0(x)$ over F_2. Therefore,

$$x^2 \equiv (b(x) + c(x))^2 \mod f_1(x)$$

Then $Hada(1, x, b(x), b(x)+ g_0(x))$ is involutory.

Analyzing Polynomials of T

For any T of order 8 satisfying those three conditions, its minimal polynomial only has 7 choices. They are:

$f_1(x)=x^8+x+1$, $f_2(x)=x^8+x^2+1$, $f_3(x)=x^8+x^3+1$,
$f_4(x)=x^8+x^4+1$, $f_5(x)=x^8+x^5+1$, $f_6(x)=x^8+x^6+1$,
$f_7(x)=x^8+x^7+1$

For each $f_k(x)$, we compute all $g(x)$ satisfying the following equation

$$x^2 \equiv (g(x))^2 \mod f_k(x) \qquad (1)$$

Algorithm 2

With $f_1(x)=x^8+x+1$, the equation (1) has 16 solutions. They are

$$g_1(x), g_2(x),\ldots, g_{16}(x).$$

Algorithm 2:

Step 1: Search $b(x)$ over $F_2[x]/(f_1(x))$

Step 2: k from 1 to 16, construct involutory Hadamard matrix

$$Hada(\ 1, x, b(x), b(x)+g_k(x)\ )$$

Step 3: If the matrix is MDS, then output the result

$$Hada(\ 1, T, b(T), b(T)+g_k(T)\ )$$

and its XORs.

Comparisons with LW16 (FSE2016)

Entries are matrices of order 8.

Matrix type	Sum of XORs	Number of results	Running time	Ref.
Involutory $Hada(I, A, A^{-1}, A+A^{-1})$	40	80640	1 day	LW16
Involutory $Hada(I, A, B, C)$	20	40320	1’ 04”	Ours

LW16 (FSE2016) platform: Magma v2.20-3 Intel Core i5

Our platform: C-free Intel Core i5-5300U 4G 2.30GHz

Comparisons---Lightweight Involutory Hadamard MDS Matrix

Matrix type	Entries	Sum of XORs	Ref.
$Hada(I, A, A^{-1}, A+A^{-1})$	$GL(4, F_2)$	24	LW16
$Hada(0x1, 0x4, 0x9, 0xd)$	$F_{2^4} / 0x13$	24	JNP14, SKOP15
$Hada(0x1, 0x2, 0x6, 0x4)$	$F_{2^4} / 0x19$	24	ABBLM14
$Hada(I, A, B, C)$	$F_2[T_{4\times4}]$	24	Ours
$Hada-cauchy(0x01, 0x02, 0xfc, 0xfe)$	$F_{2^8} / 0x11b$	296	CG14
$Hada(0x01, 0x02, 0x04, 0x06)$	$F_{2^8} / 0x11d$	88	BR00
$Hada(0x01, 0x02, 0xb0, 0xb2)$	$F_{2^8} / 0x165$	64	SKOP15
$Subfield-Hada(0x1, 0x4, 0x9, 0xd)$	$F_{2^4} / 0x13$	48	SKOP15
$Hada(I, A, A^{-1}, A+A^{-1})$	$GL(8, F_2)$	40	LW16
$Hada(I, A, B, C)$	$F_2[T_{8\times8}]$	20	Ours

Thank you for your attention!