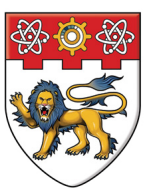
Lightweight MDS Generalized Circulant Matrices

Meicheng Liu[1,2] Siang Meng Sim[1]

1.Nanyang Technological University, Singapore

2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, P. R. China

Fast Software Encryption 2016
21 March 2016



NANYANG TECHNOLOGICAL UNIVERSITY

中国科学院 CHINESE ACADEMY OF SCIENCES

Table of Contents

Table of Contents

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 matrix can be quantified by branch number, $\mathcal{B}$.

- Minimum number of nonzero components of nonzero input and output vector pairs.

Branch Number of the Diffusion Matrices

Proposition

For any permutation matrices P and Q, the branch number of matrices M and PMQ are the same.

Definition

Two matrices M and M' are branch-equivalent, denoted by $M \sim_{\mathcal{B}} M'$, if there exist two permutation matrices P and Q such that $M' = PMQ$.

Branch-equivalent matrices have the same branch number.

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 the MDS matrices.

Example

The diffusion matrix in `AES`.

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

It is MDS and has a branch number of 5.

Circulant Matrices

Definition

A circulant matrix C is a square matrix of order k, where each subsequent row is a right rotation of the previous row.

$$\begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ c_3 & c_0 & c_1 & c_2 \\ c_2 & c_3 & c_0 & c_1 \\ c_1 & c_2 & c_3 & c_0 \end{pmatrix}$$

A circulant matrix can be denoted by its first row $circ(c_0, c_1, c_2, ..., c_{k-1})$.

Exhaustive Search for MDS Circulant Matrices

Choose an ordered multi-set of k elements to define the first row of a circulant matrix of order k.

- For each permutation of the multi-set, check if it is MDS. But there are up to $k!$ ways to permute the entries.
- MDS circulant matrices can have repeated entries, there are much more ways to pick a multi-set than a set of k distinct elements.

In this work, we tackle these 2 challenges through the analysis of the circulant matrix structure.

Table of Contents

Table of Contents

Challenge 1

Challenge:
For each permutation of the multi-set, check if it is MDS. But there are up to $k!$ ways to permute the entries.

Strategy:
We group the circulant matrices into equivalence classes to reduce the search space.

How it works:
An equivalence class of circulant matrices is a set of circulant matrices satisfying the branch-equivalent relation $\sim_{\mathcal{B}}$.
It is sufficient to check one representative from each equivalence classes.

Compact Equivalence Classes of Circulant Matrices

Lemma

circ$(c_0, c_1, ..., c_{k-1}) \sim_{\mathcal{B}}$ *circ*$(c_{j_0}, c_{j_1}, ..., c_{j_{k-1}})$ *if and only if* $\exists a, b \in Z_k, \gcd(b, k) = 1$ *such that* $\forall i \in \{0, 1, ..., k-1\}$, $j_i = (bi + a) \bmod k$.

Order of the Matrix	Total no. of Permutations	No. of Compact Equivalence Classes
3	6	1
4	24	3
5	120	6
6	$2^{9.49}$	$2^{5.91}$
7	$2^{12.30}$	$2^{6.91}$
8	$2^{15.30}$	$2^{10.30}$

Note that this is the most compact equivalence classes of generic circulant matrices.

Remark on Equivalence Classes of Hadamard Matrices

In [SKOP15], the authors proved that Hadamard matrices satisfying $\mathcal{H}$-permutations have the same branch number and proposed the equivalence classes of Hadamard matrices.

However, the converse was unclear.
I.e. Are there other permutations which are also branch-equivalent?

We proved that branch-equivalent Hadamard matrices must satisfy $\mathcal{H}$-permutations. Therefore, they actually found the most compact equivalence classes of generic Hadamard matrices.

Table of Contents

Challenge 2

Challenge:
MDS circulant matrices can have repeated entries, there are much more ways to pick a multi-set than a set of k distinct elements.

Strategy:
We show that only special multi-set of entries could be MDS to reduce the search space.

Types of MDS Circulant Matrices

Theorem

For MDS circulant matrices of order $k \leq 8$, its multi-set must be one of the following 5 types.

Order k	Possible multi-sets	Type 0 k distinct	Type 1 1 pair	Type 2 2 pairs	Type 3 3 pairs	Type 4 3 repeated
3	3	✓	✓			
4	5	✓	✓			
5	7	✓	✓	✓		
6	11	✓	✓	✓		
7	15	✓	✓	✓	✓	✓
8	22	✓	✓	✓	✓	✓

Note that this is a necessary condition, it does not guarantee the existence of MDS circulant matrices.

Table of Contents

Table of Contents

Generalized Circulant Matrices

For circulant matrices of order 4, the right rotation can be expressed using cycle notation $\tau = (0 \;\; 1 \;\; 2 \;\; 3)$,
i.e. $0 \to 1 \to 2 \to 3 \to 0$.

$$\begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}$$

The key observation is that same permutation is applied to each subsequent rows.

Generalized Circulant Matrices

We consider the permutation ρ to be any cycle of length k, this is to avoid repeated rows and repeating entries in a column.

For instance, let the cycle be $(0 \;\; 2 \;\; 1 \;\; 3)$, i.e. $0 \to 2 \to 1 \to 3 \to 0$.

$$\begin{pmatrix} a & b & c & d \\ d & c & a & b \\ b & a & d & c \\ c & d & b & a \end{pmatrix}$$

In group theory, using $\rho \in S_k$ as a generator forms a cyclic group of order k, where S_k is symmetric group.

Cyclic Matrices

Definition

A cyclic matrix C_ρ of order k is a matrix where each subsequent row is permutation ρ of the previous row, where ρ is a cycle of length k. It can be denoted by its first row $\mathrm{cyc}_\rho(c_0, c_1, ..., c_{k-1})$.

Problem:
There are $(k-1)!$ cycles of length k, not feasible to analyze every single cyclic matrix structures.

Table of Contents

Cyclic and Circulant Matrices

Using group theory, we find branch-equivalent relation between any arbitrary cyclic matrix structure and the circulant matrix structure.

Any cyclic matrix can always be transformed into a circulant matrix through some column permutation, and vice versa.

Example

$$\begin{pmatrix} a & b & c & d \\ d & c & a & b \\ b & a & d & c \\ c & d & b & a \end{pmatrix} \xrightarrow{C_1 \leftrightarrow C_2} \begin{pmatrix} a & c & b & d \\ d & a & c & b \\ b & d & a & c \\ c & b & d & a \end{pmatrix}$$

Hence, $\mathrm{cyc}_\rho(a, b, c, d) \sim_{\mathcal{B}} circ(a, c, b, d)$, where $\rho = (0 \quad 2 \quad 1 \quad 3)$.

Cyclic and Circulant Matrices

Theorem

Given an arbitrary cyclic matrix structure, there exists a bijection between the cyclic matrices and the circulant matrices of the same order k satisfying the relation $\sim_{\mathcal{B}}$.

We can extend our results of circulant matrices to cyclic matrices.

So why do we consider cyclic matrices?

Involutory MDS Cyclic Matrices

Cyclic matrices share the benefits of circulant matrices and can also be involutory MDS (IMDS).

It has been proven that IMDS circulant matrices do not exist. [GR14]

Branch-equivalent relation does not necessarily preserve the involution property.

In particular, the cyclic matrices where the permutation is a left rotation, so-called left-circulant matrices, can be involution and MDS simultaneously.

Table of Contents

Weight of the Diffusion Matrix

For simplicity, we adopt the simplified metric from [KPPY14].

The XOR count of a field element is the number of XOR gates needed to implement the multiplication of that element.

$$\text{XOR counts of one row} = \boxed{\sum_{i=1}^{k} \gamma_i} + (\ell - 1) \cdot n,$$

where γ_i is the XOR count of the i-th entry, n is the dimension of the field and ℓ is the number of nonzero entries in the row.

In this work, we only consider the summation of the XOR counts (the boxed term) in our comparison.

Finding Lightest MDS Matrices

Note that our analysis on cyclic matrices are generic and independent of the metric.

To find the lightest MDS left-circulant matrices of order $k \leq 8$, for all possible types of MDS cyclic matrices:

- choose a multi-set of k elements that has the lowest possible total XOR counts
- generate one representative for each equivalence class and check for MDS

If no representative matrix is MDS, pick the next lightest multi-set and repeat the process.

Lightest MDS Left-circulant Matrices

k	Type	Left-circulant matrices	XOR count
$\mathrm{GF}(2^8)$			
3	1	(0x1, 0x1, 0x2)	3
4	1	(0x1, 0x1, 0x2, 0x91)	8
5	2	(0x1, 0x1, 0x2, 0x91, 0x2)	11
6	1	(0x1, 0x2, 0xe1, 0x91, 0x1, 0x8)	18
7	3	(0x1, 0x1, 0x91, 0x2, 0x4, 0x2, 0x91)	21
8	4	(0x1, 0x1, 0x2, 0xe1, 0x8, 0xe0, 0x1, 0xa9)	30
$\mathrm{GF}(2^4)$			
3	1	(0x1, 0x1, 0x2)	1
4	1	(0x1, 0x1, 0x9, 0x4)	3
5	2	(0x2, 0x2, 0x9, 0x1, 0x9)	4
6	2	(0x1, 0x1, 0x9, 0xc, 0x9, 0x3)	12

Comparison of Lightweight MDS Matrices

k	Type	Matrices	Matrix form	XOR count
$\mathrm{GF}(2^8)$				
4	1	[KPPY14]	serial/circulant	9
4	1	our paper	left-circulant	8
6	–	PHOTON P_{288}	serial	23
6	1	our paper	left-circulant	18
8	4	WHIRLPOOL	circulant	49
8	4	our paper	left-circulant	30
$\mathrm{GF}(2^4)$				
4	–	LED	serial	4
4	1	[KPPY14]	serial/circulant	3
4	1	our paper	left-circulant	3
5	–	PHOTON P_{100}	serial	4
5	2	our paper	left-circulant	4
6	–	PHOTON P_{144}	serial	14
6	2	our paper	left-circulant	12

Finding Lightest Involutory MDS Matrices

We prove that IMDS left-circulant matrices of order 2^s do not exist, for integer s.

To find the lightest IMDS left-circulant matrices of order $k \leq 7$, we precompute the equations necessary and sufficient for involution.

Similar strategy as before, in addition we require the multi-sets to satisfy the equations for involution.

Lightest IMDS Left-circulant Matrices

k	Type	Matrices	XOR count
$\mathrm{GF}(2^8)$			
3	0	(0x5a, 0xa, 0x51)	30
4	-		
5	0	(0x1, 0x2, 0xb3, 0xbb, 0xa)	46
6	1	(0x1, 0x1, 0xb3, 0x2c, 0x4, 0x9a)	46
7	1	(0x1, 0x1, 0x8, 0x96, 0x21, 0x98, 0x26)	68
$\mathrm{GF}(2^4)$			
3	0	(0x2, 0xf, 0xc)	12
4	-		
5	0	(0x1, 0x2, 0x5, 0x4, 0x3)	14
6	-		

Lightweight IMDS Matrices of Order $k \leq 8$

In this work, we found lightweight IMDS left-circulant matrices of order 3,5,6 and 7.

In [SKOP15], the authors presented lightweight IMDS Hadamard matrices of order 4 and 8.

Together, we have a complete set of lightweight IMDS matrices of order $k \leq 8$.

Summary

- Propose the concept of compact equivalence classes for generic circulant matrices to reduce the search space.
- Present the necessary condition on the multi-set for MDS circulant matrices to reduce the search space.
- Introduce cyclic matrices which benefit from the circulant structure and can be IMDS.
- Complete the search on generic (left-)circulant matrices of order 8 which was previously believed to be infeasible.
- Provide the lightest possible (involutory) MDS left-circulant matrices of order $k \in \{3, ..., 8\}$.

Reference

[GR14]—Kishan Chand Gupta and Indranil Ghosh Ray. On Constructions of Involutory MDS Matrices for Lightweight Cryptography. In ISPEC 2014.

[KPPY14]—Khoongming Khoo, Thomas Peyrin, Axel Y. Poschmann and Huihui Yap. FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison. In CHES 2014.

[SKOP15]—Siang Meng Sim, Khoongming Khoo, Frédérique Oggier and Thomas Peyrin. Lightweight MDS Involution Matrices. In FSE 2015.

Thank you. :)