Direct Construction of Optimal Rotational-XOR Diffusion Primitives

Zhiyuan Guo[1,3] Renzhang Liu[2] Si Gao[1] Wenling Wu[1]
Dongdai Lin[2]

[1]TCA Laboratory, Institute of Software, Chinese Academy of Sciences, China

[2]Institute of Information Engineering, Chinese Academy of Sciences

[3]State Key Laboratory of Cryptology, P.O. Box 5159, Beijing

gzhyuan@msn.cn **Speaker**: Ling Song

March 6, 2018

Outline

1. Introductions and Notations
2. Basic Properties and Novel Observations
3. Possible Forms and Direct Constructions
4. Discussions and Conclusions

Diffusion Layers

- **Spreading internal dependencies**

  1. SECURITY : differential/linear cryptanalysis.
  2. EFFICIENCY: software/hardware performance.

Diffusion Layers

- **Spreading internal dependencies**
  1. SECURITY : differential/linear cryptanalysis.
  2. EFFICIENCY: software/hardware performance.

- **Measured by branch number**
  - ☞ Larger branch number means faster diffusion speed.
  - ☞ Bigger branch number implies more active S-boxes.

MDS Diffusion Layers

- From a coding theory perspective, Maximum Distance Separable (MDS) codes are quite good choices.

MDS Diffusion Layers

- From a coding theory perspective, Maximum Distance Separable (MDS) codes are quite good choices.

- There are two major ways to construct lightweight MDS diffusion layers.
  1. recursive strategy (serial-based implementation)
  2. circulant structure (round-based implementation)

Motivation

1. Hardware implementation often suffers from an area requirement.
2. Most methods need to perform an equivalent (or even exhaustive) search.

Motivation

1. Hardware implementation often suffers from an area requirement.
2. Most methods need to perform an equivalent (or even exhaustive) search.

Could we construct MDS diffusion layers directly over $(\mathbb{F}_2^b)^n$ with excellent hardware/software efficiency?

Rotational-XOR Diffusion Layers

Definition 1

Let n, b be positive integers and $\mathcal{I} \subset \{0, 1, ..., nb - 1\}$. A rotational-XOR diffusion layer determined by $\mathcal{I}$ over $(\mathbb{F}_2^b)^n$ is denoted by $M_{n,b}^{\mathcal{I}}$, which can be characterized as

$$M_{n,b}^{\mathcal{I}} \cdot \boldsymbol{x} = \bigoplus_{i \in \mathcal{I}} (\boldsymbol{x} \lll i),$$

where $\boldsymbol{x}$ is the $(n \cdot b)$-bit input vector.

Rotational-XOR Diffusion Layers

- Used as diffusion component in the symmetric-key ciphers
  - SM4, DBlock, RoadRunneR...

Rotational-XOR Diffusion Layers

- Used as diffusion component in the symmetric-key ciphers
  - SM4, DBlock, RoadRunneR...
- A specific type of circulant matrices: BIT-WISE circulant matrix
  - $M_{4,b}^{\mathcal{I}}$ can be expressed as

$$Circ(A,B,C,D) = \begin{bmatrix} A & B & C & D \\ D & A & B & C \\ C & D & A & B \\ B & C & D & A \end{bmatrix}.$$

Target

Proposition 1 [ZWFS09]

If $M_{4,8}^{\mathcal{I}}$ is an MDS matrix (i.e. $\mathcal{B}_d(M_{4,8}^{\mathcal{I}}) = 5$) for some set $\mathcal{I}$, then $|\mathcal{I}| \geq 5$.

Target

Proposition 1 [ZWFS09]

If $M^{\mathcal{I}}_{4,8}$ is an MDS matrix (i.e. $\mathcal{B}_d(M^{\mathcal{I}}_{4,8}) = 5$) for some set $\mathcal{I}$, then $|\mathcal{I}| \geq 5$.

- In addition to $M^{\mathcal{I}}_{4,8}$, this lower bound is tight for $M^{\mathcal{I}}_{4,b}$ as well.

Target

Proposition 1 [ZWFS09]

If $M^{\mathcal{I}}_{4,8}$ is an MDS matrix (i.e. $\mathcal{B}_d(M^{\mathcal{I}}_{4,8}) = 5$) for some set $\mathcal{I}$, then $|\mathcal{I}| \geq 5$.

- In addition to $M^{\mathcal{I}}_{4,8}$, this lower bound is tight for $M^{\mathcal{I}}_{4,b}$ as well.

☞

Our focus is only placed on the construction of $M^{\mathcal{I}}_{4,b}$ with $|\mathcal{I}| = 5$.

Notation (1)

- For a $b \times b$ binary matrix $A = (a_{i,j})$ where $1 \leq i, j \leq b$, we call <u>A has diagonal σ</u>, if $a_{i,j} = 1$ for all i and j such that $j - i = \sigma$.

$$\begin{array}{cc}
 & \begin{array}{cccccccc} diag(0) & & & & & & & diag(7) \end{array} \\
diag(-5) & \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\end{array}$$

Notation (2)

- If A has diagonals $\sigma_1, ..., \sigma_t$, and has no 1 at other positions, we denote

$$A = \sum_{i=1}^{t} diag(\sigma_i).$$

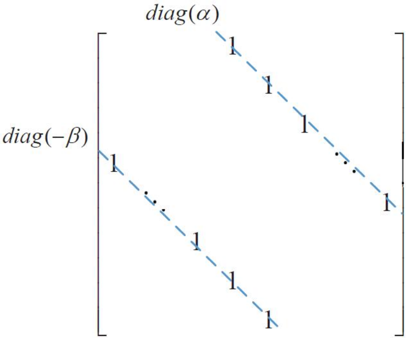
$$
\begin{array}{rl}
 & diag(0) \qquad\qquad\qquad\qquad diag(7) \\
diag(-5) & \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\end{array}
$$

Figure: $diag(7) + diag(0) + diag(-5)$

Observation (1)

Theorem 1

A $b \times b$ binary matrix $A = diag(\alpha) + diag(-\beta)$ is non-singular if and only if $(\alpha + \beta) | b$, where $\alpha, \beta > 0$,



Observation (1)

Corollary 1

For a $b \times b$ matrix $A = diag(\alpha) + diag(\beta)$, it is invertible if and only if one of the following conditions is satisfied.

(1) $\alpha \neq \beta$ and one of them is 0.

(2) $\alpha\beta < 0$ and $|\alpha - \beta|$ is a divisor of b.

Observation (2)

Proposition 2

Given an $M_{4,b}^{\mathcal{I}}$ with $\mathcal{I} = \{i_1, ..., i_5\}$, $0 \leq i_1 < \cdots < i_5 \leq 4b - 1$. Then $M_{4,b}^{\mathcal{I}'}$ and $M_{4,b}^{\mathcal{I}}$ are of the same branch number, where

$$\mathcal{I}' = \{(i_1 + b) \bmod 4b, ..., (i_5 + b) \bmod 4b\}.$$

Observation (2)

Proposition 2

Given an $M_{4,b}^{\mathcal{I}}$ with $\mathcal{I} = \{i_1, ..., i_5\}$, $0 \leq i_1 < \cdots < i_5 \leq 4b - 1$. Then $M_{4,b}^{\mathcal{I}'}$ and $M_{4,b}^{\mathcal{I}}$ are of the same branch number, where

$$\mathcal{I}' = \{(i_1 + b) \bmod 4b, ..., (i_5 + b) \bmod 4b\}.$$

Proposition 3

Given an $M_{4,b}^{\mathcal{I}}$ with $\mathcal{I} = \{i_1, ..., i_5\}$, $0 \leq i_1 < \cdots < i_5 \leq 4b - 1$. Then $M_{4,b}^{\mathcal{I}'}$ and $M_{4,b}^{\mathcal{I}}$ are of the same branch number, where

$$\mathcal{I}' = \{(4b - i_1) \bmod 4b, ..., (4b - i_5) \bmod 4b\}.$$

Observation (3)

Throughout this paper, we always assume that $M^{\mathcal{I}}_{4,b}$ contains at least one *diagonal 0* among the five non-negative diagonals.

Observation (3)

Throughout this paper, we always assume that $M^{\mathcal{I}}_{4,b}$ contains at least one *diagonal 0* among the five non-negative diagonals.

Theorem 2

For an MDS $M^{\mathcal{I}}_{4,b} = Circ(A, B, C, D)$ containing at least one diagonal 0 among the five non-negative diagonals, there always exists an

$$M^{\mathcal{I}'}_{4,b} = Circ(A', B', C', D')$$

where $A' = diag(\sigma) + diag(0)$, $\sigma > 0$, such that $\mathcal{B}_d(M^{\mathcal{I}'}_{4,b}) = \mathcal{B}_d(M^{\mathcal{I}}_{4,b})$.

Observation (4)

Theorem 3

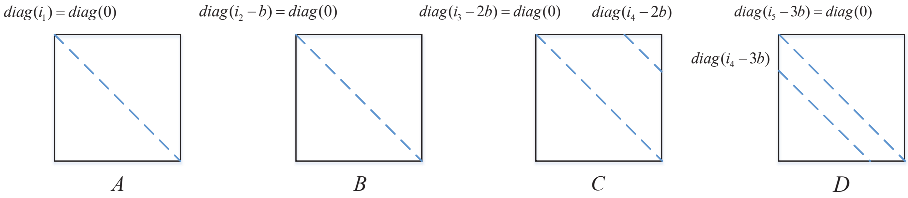
For any rotational-XOR MDS diffusion layer $M_{4,b}^{\mathcal{I}}$ with $|\mathcal{I}| = 5$, there are at most two indices in $\mathcal{I} = \{i_1, ..., i_5\}$ divisible by b.

Observation (4)

Theorem 3

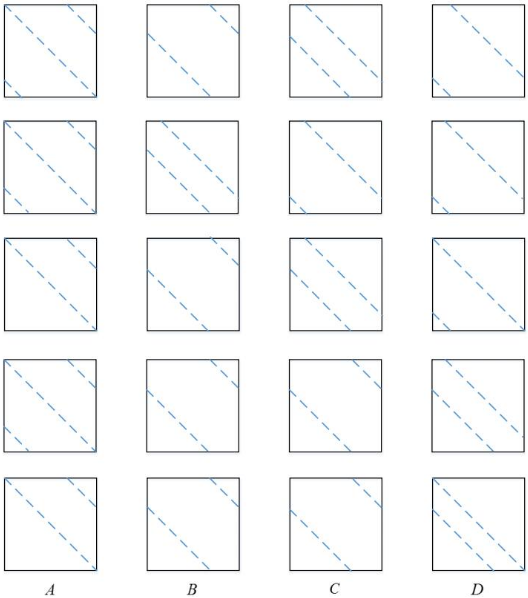
For any rotational-XOR MDS diffusion layer $M_{4,b}^{\mathcal{I}}$ with $|\mathcal{I}| = 5$, there are at most two indices in $\mathcal{I} = \{i_1, ..., i_5\}$ divisible by b.

Counterexample $\Rightarrow$

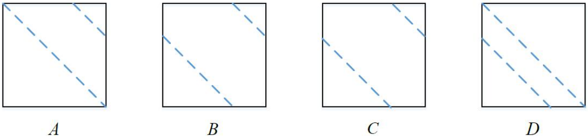


Let $(\boldsymbol{y_1}, \boldsymbol{y_2}, \boldsymbol{y_3}, \boldsymbol{y_4}) = Circ(A, B, C, D) \cdot (\boldsymbol{e_1}, \boldsymbol{e_1}, \boldsymbol{0}, \boldsymbol{0})^T$, $\boldsymbol{e_1} = (1, 0, ..., 0)$.

Four Blocks in the First Row for Each Possible Form



The Only Possible Form of MDS $M_{4,b}^{\mathcal{I}}$



Theorem 4

Any rotational-XOR MDS diffusion layer $M_{4,b}^{\mathcal{I}}$, with $|\mathcal{I}| = 5$ and $i_1 = 0$, must satisfy that

$$\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$$

for some $0 < l < b$ from a equivalent point of view.

Direct Construction (1)

Alternatively, $M_{4,b}^{\mathcal{I}}$ with $\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$ can be represented as

$$Circ(A, B, B, A+B),$$

where $A = diag(0) + diag(l)$, $B = diag(l) + diag(l-b)$.

Direct Construction (1)

Alternatively, $M_{4,b}^{\mathcal{I}}$ with $\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$ can be represented as

$$Circ(A, B, B, A+B),$$

where $A = diag(0) + diag(l)$, $B = diag(l) + diag(l-b)$.

Theorem 5

Let $M = Circ(A, B, B, A+B)$, where $A, B, A+B \in GL(b, \mathbb{F}_2)$. M is MDS if and only if the following three statements hold.

(1) $|A + B + BA^{-1}B| \neq 0$.
(2) $|A + B + BA^{-1}BA^{-1}B| \neq 0$.
(3) $|A + BA^{-1}B + BA^{-1}BA^{-1}B| \neq 0$.

Direct Construction (2)

Taking the statement (2) as an example, we deduce the sufficient and necessary condition as follows.

Theorem 6

Suppose $A = diag(0) + diag(l)$ and $B = diag(l) + diag(l - b)$ are two $b \times$b binary matrices, where $0 < l < b$. Then $|A + B + BA^{-1}BA^{-1}B|$ is non-zero if and only if $l \neq 3b \bmod 7$.

Proof of Theorem 6

- $|A+B+BA^{-1}BA^{-1}B| \neq 0 \Leftrightarrow |I+A^{-1}B+A^{-1}BA^{-1}BA^{-1}B| \neq 0.$
- Let $W = A^{-1}B$, then
$$I + A^{-1}B + A^{-1}BA^{-1}BA^{-1}B = I + W + W^3.$$
- For any eigenvalue of W, denoted by λ, it satisfies
$$|\lambda I - U| = 0 \Leftrightarrow \lambda^b + (\lambda+1)^{b-l} = 0.$$
- $I + W + W^3$ is non-singular if and only if $1+\lambda+\lambda^3 \neq 0$. Consider the conditions for $1+\lambda+\lambda^3 = 0$. Notice $1+\lambda+\lambda^3$ is a primitive polynomial of order 7 over $\mathbb{F}_2$.
$$\lambda^b + (\lambda+1)^{b-l} = 0 \Leftrightarrow \lambda^b + \lambda^{3(b-l)} = 0 \Leftrightarrow b = 3(b-l) \bmod 7,$$
which is equivalent to $l = 3b \bmod 7$.

Construction of MDS $M^{\mathcal{I}}_{4,b} = Circ(A, B, B, A + B)$

Theorem 7

Assume $A = diag(0) + diag(l)$ and $B = diag(l) + diag(l - b)$ are two $b\times$b binary matrices. Then $M^{\mathcal{I}}_{4,b}$, denoted by $Circ(A, B, B, A + B)$, is MDS, if and only if all conditions below are fulfilled.

(1) $l \neq 2b$ mod 3.

(2) $l \neq 3b$ mod 7.

(3) $l \neq 5b$ mod 7.

Hardware Efficiency

- All rows for a circulant/ Hadamard matrix are equivalent in terms of XOR count, so we use the amount of XORs required to evaluate the first row to evaluate the lightweightness.

Matrix type	Elements	The first row	XOR count	Reference
Hadamard	$\mathbb{F}_{2^4}/0x13$	$(0x01, 0x02, 0x08, 0x09)$	17	[SKOP15]
Hadamard	$GL(4, \mathbb{F}_2)$	(I, A, B, C)	16	[LW16]
Circulant	$GL(4, \mathbb{F}_2)$	(I, I, A, B)	15	[LW16]
Circulant	$\mathbb{F}_{2^4}/0x13$	$(0x01, 0x01, 0x09, 0x04)$	15	[LS16]
Circulant	$\mathbb{F}_{2^4}/0x13$	$(0x01, 0x01, 0x04, 0x09)$	15	[KPPY14]
Circulant	$GL(4, \mathbb{F}_2)$	$(A, B, B, A+B)$	16	This paper
Circulant	$\mathbb{F}_{2^8}/0x11b$	$(0x02, 0x03, 0x01, 0x01)$	38	[DR02]
Hadamard	$\mathbb{F}_{2^8}/0x1c3$	$(0x01, 0x02, 0x04, 0x91)$	37	[SKOP15]
Circulant	$\mathbb{F}_{2^8}/0x11b$	$(0x01, 0x01, 0x04, 0x8e)$	33	[KPPY14]
Circulant	$\mathbb{F}_{2^8}/0x1c3$	$(0x01, 0x01, 0x02, 0x91)$	32	[LS16]
Circulant	$GL(8, \mathbb{F}_2)$	(I, I, A, B)	27	[LW16]
Circulant	$GL(8, \mathbb{F}_2)$	$(A, B, B, A+B)$	32	This paper

Software Performance

Our construction favors implementations with nb-bit processors.

- For any 32×32 binary matrix in that table, computing a 32-bit output requires 4 XORs and 4 rotations, with no extra memory cost.

Software Performance

Our construction favors implementations with nb-bit processors.

- For any 32×32 binary matrix in that table, computing a 32-bit output requires 4 XORs and 4 rotations, with no extra memory cost.
    - Since many 32-bit processors have built-in rotation instructions, performing such transformation takes only 8 instructions.
    - However, other examples in that table take at least 3×4 XORs, no matter how multiplication operation is implemented.

Conclusion

- Once given the block size b, the set of candidates for l is therewith determined:

$$\Lambda = \{l | 0 < l < b, l \neq 2b \bmod 3, l \neq 3b \bmod 7, l \neq 5b \bmod 7\}.$$

So an arbitrary $l \in \Lambda$ corresponds to a perfect diffusion layer $M_{4,b}^{\mathcal{I}}$, where $\mathcal{I} = \{0, l, l + b, l + 2b, 3b\}$.

Conclusion

- Once given the block size b, the set of candidates for l is therewith determined:

$$\Lambda = \{l | 0 < l < b, l \neq 2b \bmod 3, l \neq 3b \bmod 7, l \neq 5b \bmod 7\}.$$

  So an arbitrary $l \in \Lambda$ corresponds to a perfect diffusion layer $M_{4,b}^{\mathcal{I}}$, where $\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$.

- This strategy provides a quite comprehensive solution to designing such 4×4 MDS matrices.

Conclusion

- Once given the block size b, the set of candidates for l is therewith determined:

$$\Lambda = \{l | 0 < l < b, l \neq 2b \bmod 3, l \neq 3b \bmod 7, l \neq 5b \bmod 7\}.$$

So an arbitrary $l \in \Lambda$ corresponds to a perfect diffusion layer $M_{4,b}^{\mathcal{I}}$, where $\mathcal{I} = \{0, l, l+b, l+2b, 3b\}$.

- This strategy provides a quite comprehensive solution to designing such 4×4 MDS matrices.

- It is the first time that lightweight rotational-XOR MDS matrices have been constructed without any auxiliary search.

Thanks for your attention !