FSE 2020

Finding Bit-Based Division Property for Ciphers with Complex Linear Layers

Kai Hu [1]   Qingju Wang [2]   Meiqin Wang [1]

[1]School of Cyber Science and Technology, Shandong University

[2]SnT, University of Luxembourg

November 1, 2020

Outline

Main Result

- A new model of the propagation of division trails over a complex linear layer used in the automatic search for the bit-based division property (BDP)

$$\begin{cases} wt(\boldsymbol{u}) = wt(\boldsymbol{v}) \\ E(i,j) \cdot v_i = \sum_{k=0}^{n-1} M(i,k) \cdot v_i \cdot u_k \cdot M_{\boldsymbol{v},\boldsymbol{u}}^{\text{expand}'}(k,j), \text{ for } 0 \leqslant i,j \leqslant n-1 \end{cases}$$

- Universal & precise
- Results for AES, LED-64, CLEFIA and Camellia

Bit-Based Division Property and Division Trail

Conventional Bit-Based Division Property [TM,FSE 2016]

Let $\mathbb{X}$ be a multiset and $\mathbb{K}$ be a set and their elements are chosen from $\mathbb{F}_2^n$, When $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^n$, it fulfills the following conditions for any $\boldsymbol{u} \in \mathbb{F}_2^n$:

$$\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \begin{cases} \mathit{unknown}, & \text{if there exists a } \boldsymbol{k} \in \mathbb{K} \text{ s.t. } \boldsymbol{u} \succeq \boldsymbol{k} \\ 0, & \text{otherwise} \end{cases}.$$

where $\pi_{\boldsymbol{u}}(\boldsymbol{x}) = \prod_i x_i^{u_i}$ and $\boldsymbol{u} \succeq \boldsymbol{k}$ means $u_i \geqslant k_i$ for i.

Bit-Based Division Property and Division Trail

Conventional Bit-Based Division Property [TM,FSE 2016]

Let $\mathbb{X}$ be a multiset and $\mathbb{K}$ be a set and their elements are chosen from $\mathbb{F}_2^n$, When $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^n$, it fulfills the following conditions for any $\boldsymbol{u} \in \mathbb{F}_2^n$:

$$\bigoplus_{\boldsymbol{x} \in \mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \begin{cases} \textit{unknown}, & \text{if there exists a } \boldsymbol{k} \in \mathbb{K} \text{ s.t. } \boldsymbol{u} \succeq \boldsymbol{k} \\ 0, & \text{otherwise} \end{cases} .$$

where $\pi_{\boldsymbol{u}}(\boldsymbol{x}) = \prod_i x_i^{u_i}$ and $\boldsymbol{u} \succeq \boldsymbol{k}$ means $u_i \geqslant k_i$ for i.

Division Trail [XZBL, ASIACRYPT 2016]

Assume the initial division property of a cipher be $\mathbb{K}_0 \overset{def}{=} \mathcal{D}_{\mathbb{K}_0}$, and the division property after the i-th round is $\mathbb{K}_i \overset{def}{=} \mathcal{D}_{\mathbb{K}_i}$. We have a trail of r rounds of division property propagations

$$\{\boldsymbol{k}\} \overset{\text{def}}{=} \mathbb{K}_0 \to \mathbb{K}_1 \to \mathbb{K}_2 \to \cdots \to \mathbb{K}_r.$$

For $(\boldsymbol{k}_0, \boldsymbol{k}_1, \ldots, \boldsymbol{k}_r) \in (\mathbb{K}_0 \times \mathbb{K}_1 \times \cdots \times \mathbb{K}_r)$, if $\boldsymbol{k}_i$ can propagate to $\boldsymbol{k}_{i+1}$ for all $i \in \{0, 1, \ldots, r-1\}$, we call $(\boldsymbol{k}_0 \to \boldsymbol{k}_1 \to \cdots \to \boldsymbol{k}_r)$ an r-round division trail.

Trace the Propagation of Division Trails

MILP/SAT-Aided Method [XZBL, ASIACRYPT 2016]

- Create an MILP/SAT model $\mathcal{M}$ according to the propagation rules of division property and let the solutions be valid division trails like

  $\boldsymbol{k}_0 \to \boldsymbol{k}_1 \to \boldsymbol{k}_2 \cdots \to \boldsymbol{k}_{r-1} \to \boldsymbol{k}_r.$
- If $\boldsymbol{k}_0 \to \cdots \to \boldsymbol{e}_j$ is infeasible, the j-th bit is zero-sum.

Trace the Propagation of Division Trails

MILP/SAT-Aided Method [XZBL, ASIACRYPT 2016]

- Create an MILP/SAT model $\mathcal{M}$ according to the propagation rules of division property and let the solutions be valid division trails like

  $$\boldsymbol{k}_0 \to \boldsymbol{k}_1 \to \boldsymbol{k}_2 \cdots \to \boldsymbol{k}_{r-1} \to \boldsymbol{k}_r.$$

- If $\boldsymbol{k}_0 \to \cdots \to \boldsymbol{e}_j$ is infeasible, the j-th bit is zero-sum.

Propagation Rules

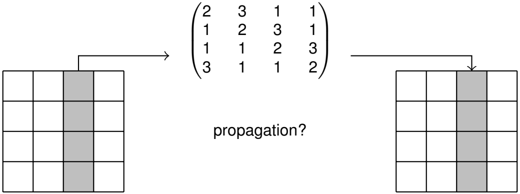
- For a vectorial Boolean function $\boldsymbol{f} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ sending $\boldsymbol{x}$ to $\boldsymbol{y}$, $\boldsymbol{u} \to \boldsymbol{v}$ is a valid division trail for $\boldsymbol{f}$ iff there exists $\boldsymbol{u}' \succeq \boldsymbol{u}$ satisfying that $\pi_{\boldsymbol{u}'}(\boldsymbol{x})$ is a monomial of $\pi_{\boldsymbol{v}}(\boldsymbol{y})$.
- The propagation rules for *XOR*, *COPY*, *AND*, *SBOX* have been well modeled.
- The complex linear layer has not been modeled perfectly.

Motivation

Why We Focus on the Complex Linear Layer?

- Many important ciphers take a complex linear layer as the diffusion layer

  e.g., AES, CLEFIA take MDS matrices
- BDP is currently the most effective method to find integral distinguishers
- No perfect method to evaluate the security of the ciphers with complex linear layers against BDP



Previous Works

$\mathcal{S}$ Method: Universal & Imprecise [SWW, IET]

- Basic idea: represent the matrix-multiplication by COPY and XOR

$$\texttt{For}\ \ \boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1}) \xrightarrow{M} \boldsymbol{y} = (y_0, y_1, \ldots, y_{n-1}),$$
$$x_j \xrightarrow{COPY} (t_{0,j}, t_{1,j}, \ldots, t_{n-1,j}), (t_{i,0}, t_{i,1}, \ldots, t_{i,n-1}) \xrightarrow{XOR} y_i$$

- Advantage: any linear layer can be modeled
- Disadvantage: some balanced bits could be missed

$\mathcal{ZR}$ Method: Precise & Restricted [ZR, IET]

- Basic idea: a valid trail iff the corresponding sub-matrix is invertible
- Advantage: trace each valid trial precisely
- Disadvantage: applicable to binary matrices, e.g. $M_{SKINNY} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

Contribution of This Paper.

Contribution 1: A Universal & Precise Model

- Precisely applicable to non-binary matrices

  `model the MDS matrix: prove 5-round AES has no BDP`
- Precisely applicable to non-invertible matrices

  `reproduce the key-dependent dist. of 5-round AES`

Contribution 2: New & Better BDP

- 7-round integral distinguisher for LED, the longest
- 6-round BDP for Misty & new 6-round BDP for Misty with 62 active bits
- 10-round BDP for CLEFIA
- 7-round BDP for Camellia

Overview of Our New Model

⚠ If not stated explicitly, we always assume $wt(\boldsymbol{u}) = wt(\boldsymbol{v})$.

Proposition

For a primitive matrix $M \in \mathbb{F}_2^{n\times n}$ [1], a division trail $(\boldsymbol{u}, \boldsymbol{v})$ is valid iff $(\boldsymbol{u}, \boldsymbol{v})$ meets the following constraints

$$E(i,j) \cdot v_i - \sum_{k=0}^{n-1} M(i,k) \cdot v_i \cdot u_k \cdot M_{\boldsymbol{v},\boldsymbol{u}}^{\text{expand}'}(k,j) = 0, \ \textit{for}\ 0 \leqslant i,j \leqslant n-1,$$

where E is a $n \times n$ identity matrix and $M_{\boldsymbol{v},\boldsymbol{u}}^{\text{expand}'} \in \mathbb{F}_2^{n\times n}$ is an auxiliary matrix with n^2 elements.

To model $M \in F_2^{n\times n}$, we need totally
n^2 4-degree constraints with n^2 auxiliary variables denoting $M_{n\times n}^{expand'}$

[1] $M' \in \mathbb{F}_2^{ms\times ms}$ is the primitive matrix of $M \in \mathbb{F}_{2^m}^{s\times s}$ if M' and M is equivalent except they are defined over different linear spaces.

Starting Point of the New Model

Theorem (Zhang & Rijmen)

Let M be the $n \times n$ primitive matrix of an invertible linear transformation and $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n$. Then $\boldsymbol{u} \xrightarrow{M} \boldsymbol{v}$ is one of the valid division trails of the linear transform M iff $M_{\boldsymbol{v},\boldsymbol{u}}$ [2] *is invertible.*

Example. We check whether $\boldsymbol{u} = (0,1,1,0) \rightarrow \boldsymbol{v} = (0,1,1,0)$ is valid.

$$\begin{array}{cc} & \begin{bmatrix} 0 & 0 & 1 & 1 \end{bmatrix} \\ \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} \end{array} \qquad \begin{bmatrix} a_{1,2} & a_{1,3} \\ a_{2,2} & a_{2,3} \end{bmatrix}$$

$M_{\boldsymbol{v},\boldsymbol{u}}$ is invertible iff $\boldsymbol{u} \rightarrow \boldsymbol{v}$ is valid

---

[2] $M_{v,u} = \{M(i,j)\}_{wt(\boldsymbol{v}) \times wt(\boldsymbol{u})}, v_i = 1, u_j = 1.$

Basic Idea

Common Knowledge

$M_{\boldsymbol{v},\boldsymbol{u}}$ is invertible $\Longleftrightarrow M_{\boldsymbol{v},\boldsymbol{u}} M_{\boldsymbol{v},\boldsymbol{u}}^{-1} = E_{wt(\boldsymbol{v})\times wt(\boldsymbol{v})}$ [3] has solutions.

Challenge

- The exact $\boldsymbol{u}$, $\boldsymbol{v}$ and their hamming weights are not known in advance
- The exact size of $M_{\boldsymbol{v},\boldsymbol{u}}$ is not known
- When declaring the variables, the size is always required by the SAT/MILP tools

[3] $E_{wt(\boldsymbol{v})\times wt(\boldsymbol{v})}$ is a $wt(\boldsymbol{v}) \times wt(\boldsymbol{v})$ identity matrix, if not ambiguous, denoted by E.

Compute the Expanded Matrix of $M_{\boldsymbol{v},\boldsymbol{u}}$

Definition (Expanded Matrix)

Given a primitive matrix $M \in \mathbb{F}_2^{n\times n}$ and one of its sub-matrix $M_{\boldsymbol{v},\boldsymbol{u}}$, the expanded matrix $M^{\text{expand}}_{\boldsymbol{v},\boldsymbol{u}} \in \mathbb{F}_2^{n\times n}$ of $M_{\boldsymbol{v},\boldsymbol{u}}$ is defined as

$$M^{\text{expand}}_{\boldsymbol{v},\boldsymbol{u}}(i,j) = \begin{cases} M(i,j), & \text{if } v_i = 1 \text{ and } u_j = 1, \\ 0, & \text{otherwise.} \end{cases}$$

$$\begin{array}{cc} & \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} \end{array} \longrightarrow \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & a_{1,1} & a_{1,2} & 0 \\ 0 & a_{2,1} & a_{2,2} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

The size of $M^{\text{expand}}_{\boldsymbol{v},\boldsymbol{u}}$ is fixed $\Rightarrow$ use `ARRAY(index, value)` to declare it

Check the Invertibility of $M_{\boldsymbol{v},\boldsymbol{u}}$

Constrain $M_{\boldsymbol{v},\boldsymbol{u}}^{\text{expand}}$ & Ensure $M_{\boldsymbol{v},\boldsymbol{u}}$ is invertible

Theorem

Let M be a matrix in $\mathbb{F}_2^{n\times n}$. $M_{\boldsymbol{v},\boldsymbol{u}}$ is invertible iff $M_{\boldsymbol{v},\boldsymbol{u}}^{\text{expand}} M_{\boldsymbol{v},\boldsymbol{u}}^{\text{expand}'} = E_{\boldsymbol{v}}$ has solutions, where $E_{\boldsymbol{v}} \in \mathbb{F}_2^{n\times n}$ is defined as follows,

$$E_{\boldsymbol{v}}(i,j) = \begin{cases} 1, & \text{if } i = j \text{ and } v_i = 1 \\ 0, & \text{else} \end{cases} .$$

Proof.

w.l.o.g assume $M_{\boldsymbol{v},\boldsymbol{u}}$ is located in the top-left corner of M (also $M_{\boldsymbol{v},\boldsymbol{u}}^{\text{expand}}$).

$$\left[\begin{array}{c|c} M_{\boldsymbol{v},\boldsymbol{u}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right] \cdot \left[\begin{array}{c|c} X_{0,0} & X_{0,1} \\ \hline X_{1,0} & X_{1,1} \end{array}\right] = \left[\begin{array}{c|c} E & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right] \Leftrightarrow \begin{cases} M_{\boldsymbol{v},\boldsymbol{u}} \cdot X_{0,0} = E \\ M_{\boldsymbol{v},\boldsymbol{u}} \cdot X_{0,1} = \mathbf{0} \end{cases}$$

□

The Compact Algorithm

Observation

$M^{\text{expand}}_{\boldsymbol{v},\boldsymbol{u}}$ can be generated by the following formula,

$$M^{\text{expand}}_{\boldsymbol{v},\boldsymbol{u}}(i,j) = M(i,j)\cdot v_i \cdot u_j.$$

Observation

The matrix E_v can be generated by the following formula,

$$E_{\boldsymbol{v}}(i,j) = E(i,j)\cdot v_i.$$

Where E is the $wt(\boldsymbol{v}) \times wt(\boldsymbol{v})$ identity matrix.

Put Things Together

$$E(i,j)\cdot v_i = \sum_{k=0}^{n-1} M(i,k)\cdot v_i \cdot u_k \cdot M^{\text{expand}'}_{\boldsymbol{v},\boldsymbol{u}}(k,j), \text{ for } 0 \leqslant i,j \leqslant n-1.$$

Remove Invertible Condition of Theorem in [ZR, IET]

It was stated in [ZR, IET] that M should be invertible

Theorem

Let M be the $p \times q$ primitive matrix of a linear transformation. For $\boldsymbol{u} \in \mathbb{F}_2^q$ and $\boldsymbol{v} \in \mathbb{F}_2^p$, $\boldsymbol{u} \xrightarrow{M} \boldsymbol{v}$ is a valid division trail of the linear layer M if and only if $M_{\boldsymbol{v},\boldsymbol{u}}$ is invertible.

M can be non-square let alone non-invertible

Proof.

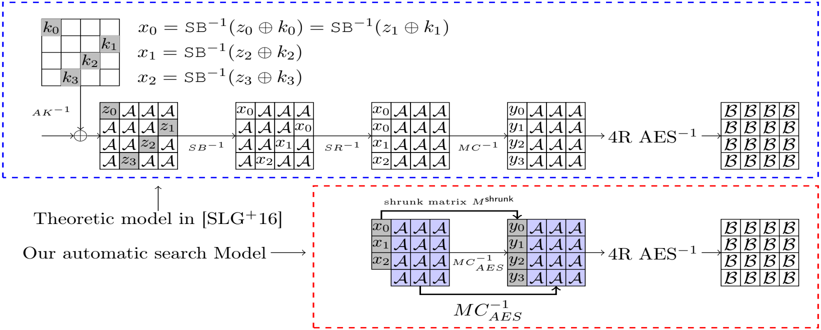
In [ZR, IET], the invertibility of M is only used to prove $wt(\boldsymbol{u}) = wt(\boldsymbol{v})$. Discussion case-by-case.

- $wt(\boldsymbol{u}) > wt(\boldsymbol{v})$ is impossible because M is a linear mapping.
- If $wt(\boldsymbol{u}) < wt(\boldsymbol{v})$, $\boldsymbol{v}$ is redundant.

□

Reproduce the Key-Dependent Integral Distinguisher

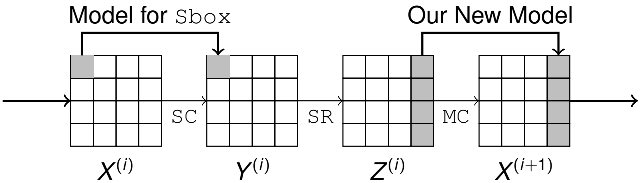
- Prepare a shrunk matrix to satisfy the input condition
- The shrunk matrix cannot be handled by $\mathcal{S}$ or $\mathcal{ZR}$ method



$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{bmatrix} \begin{bmatrix} x_0 \\ x_0 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} E \oplus B & D & 9 \\ 9 \oplus E & B & D \\ D \oplus 9 & E & B \\ B \oplus D & 9 & E \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 5 & D & 9 \\ 7 & B & D \\ 4 & E & B \\ 6 & 9 & E \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} \triangleq M^{\text{shrunk}}$$

The Longest BDP of LED-64

Round function of LED:



New and the longest BDP:

$$\begin{bmatrix} \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{C} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{C} \\ \mathcal{C} & \mathcal{A} & \mathcal{A} & \mathcal{A} \end{bmatrix} \xrightarrow{6R} \begin{bmatrix} \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \end{bmatrix}, \begin{bmatrix} \mathcal{A} & \texttt{aaac} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \end{bmatrix} \xrightarrow{7R} \begin{bmatrix} \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \end{bmatrix}$$

BDP of MISTY1

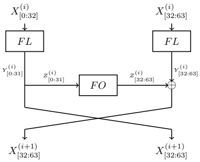
- BDP & existing word-Based DP:

$$\begin{bmatrix} \texttt{caaa} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \end{bmatrix} \xRightarrow{6R} \begin{bmatrix} \mathcal{B} & \texttt{bbb?} & ? & ? \\ ? & ? & ? & ? \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \end{bmatrix}$$

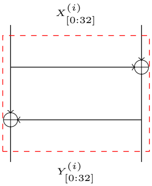
- New 6-r BDP with 62 active bits:

$$\begin{bmatrix} \texttt{ccaa} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \end{bmatrix} \xRightarrow{6R} \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \end{bmatrix}$$

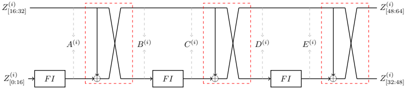
Functions of MISTY1:



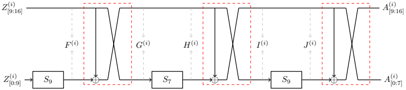
(a) Structure of MISTY1.



(b) FL function.



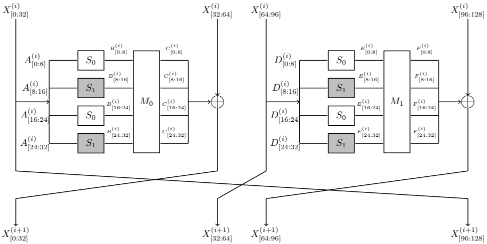
(c) FO function.



(d) FI function.

BDP of CLEFIA

- functions of CLEFIA:

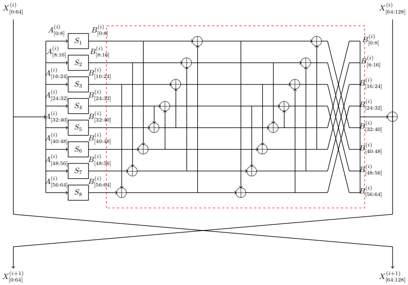


- BDP & word-based DP:

$$\begin{bmatrix} \mathtt{caaaaaaa} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \end{bmatrix} \xRightarrow{10R} \begin{bmatrix} ? & ? & ? & ? \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ ? & ? & ? & ? \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \end{bmatrix}.$$

BDP of Camellia

functions of CLEFIA:



new and the longest BDP (with FL/FL^{-1} located after the first round):

$$\begin{bmatrix} \mathtt{caaaaaaa} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{A} & \mathcal{A} & \mathcal{A} \end{bmatrix} \xrightarrow{7R} \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \\ \mathcal{B} & \mathcal{B} & \mathcal{B} & \mathcal{B} \end{bmatrix}.$$

Summary

Main results:

- A new and effective SAT model to describe the division property propagation over a complex linear layer, which can be used in MDS and any other kinds of matrix.
- Remove the invertible condition from $\mathcal{ZR}$ method, making it universal even for non-square matrices.
- Reproduce or find new integral distinguishers for many important ciphers.

Suggestion:

- Binary matrix: ours & $\mathcal{ZR}$ method
- Non-binary matrix with size $n \leq 64$: ours
- Non-binary matrix with size $n \geqslant 64$: $\mathcal{S}$ method

Thanks for your attention!