Using MILP in Analysis of Feistel Structures

and Improving Type II GFS by Switching Mechanism

Mahdi Sajadieh and Mohammad Vaziri

Indocrypt 2018

Table of Contents

Background

- Feistel structures form a significant category of block ciphers.

Background

- Feistel structures form a significant category of block ciphers.
- Two methods for improving the immunity of Feistel structures:

Background

- Feistel structures form a significant category of block ciphers.
- Two methods for improving the immunity of Feistel structures:
  1. Switching Mechanism.

Background

- Feistel structures form a significant category of block ciphers.
- Two methods for improving the immunity of Feistel structures:
  1. Switching Mechanism.
  2. Changing permutations of sub-blocks.

Results

- A technique to count the active S-boxes is proposed by relying on:

Results

- A technique to count the active S-boxes is proposed by relying on:
  1. MILP method.

Results

- A technique to count the active S-boxes is proposed by relying on:
  1. MILP method.
  2. Summation representation method.

Results

- A technique to count the active S-boxes is proposed by relying on:
  1. MILP method.
  2. Summation representation method.
- Improving Shibutani's results at SAC 2010.

Results

- A technique to count the active S-boxes is proposed by relying on:
  1. MILP method.
  2. Summation representation method.
- Improving Shibutani's results at SAC 2010.
- Extraction new inequalities related to multiple MDS matrices.

Results

- A technique to count the active S-boxes is proposed by relying on:
  1. MILP method.
  2. Summation representation method.
- Improving Shibutani's results at SAC 2010.
- Extraction new inequalities related to multiple MDS matrices.
- Given some results related to linear cryptanalysis.

Table of Contents

GFS Structures

GFS Structures

- Relation

GFS Structures

- Relation

$$(X_0, X_1, ..., X_{l-1}) \rightarrow \pi(X_0, F_0(X_0) \oplus X_1, X_2, F_1(X_2) \oplus X_3, ..., F_{l/2-1}(X_{l-2}) \oplus X_{l-1})$$

GFS Structures

- Relation

  $(X_0, X_1, ..., X_{l-1}) \rightarrow \pi(X_0, F_0(X_0) \oplus X_1, X_2, F_1(X_2) \oplus X_3, ..., F_{l/2-1}(X_{l-2}) \oplus X_{l-1})$

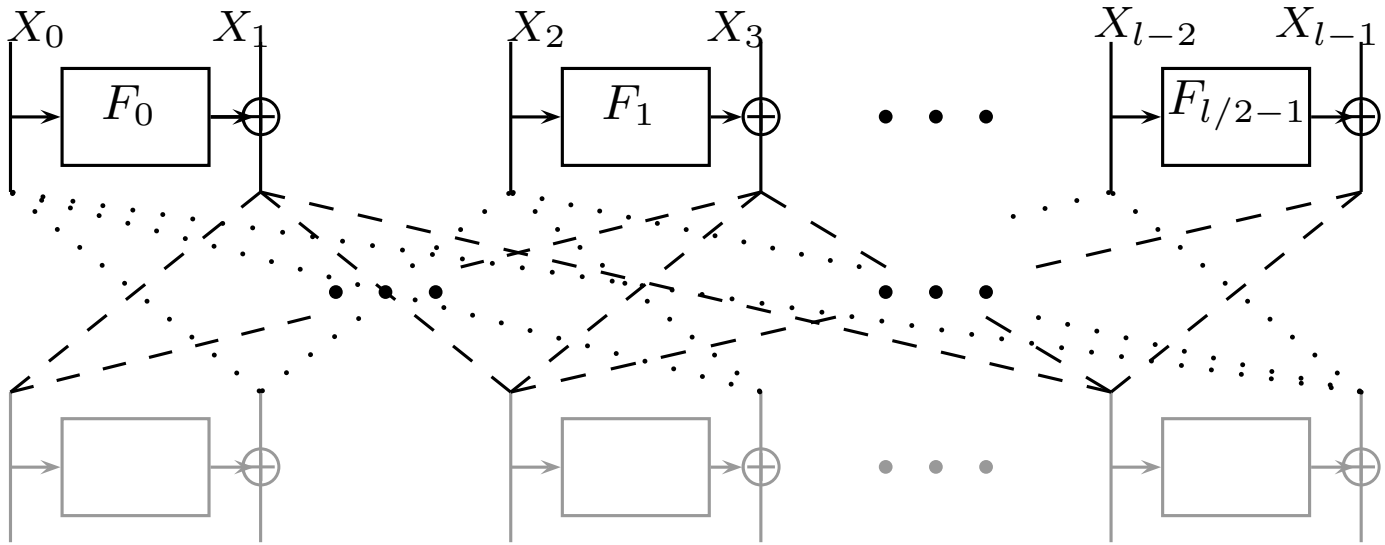
- Figure

GFS Structures

- Relation

$$(X_0, X_1, ..., X_{l-1}) \rightarrow \pi(X_0, F_0(X_0) \oplus X_1, X_2, F_1(X_2) \oplus X_3, ..., F_{l/2-1}(X_{l-2}) \oplus X_{l-1})$$

- Figure

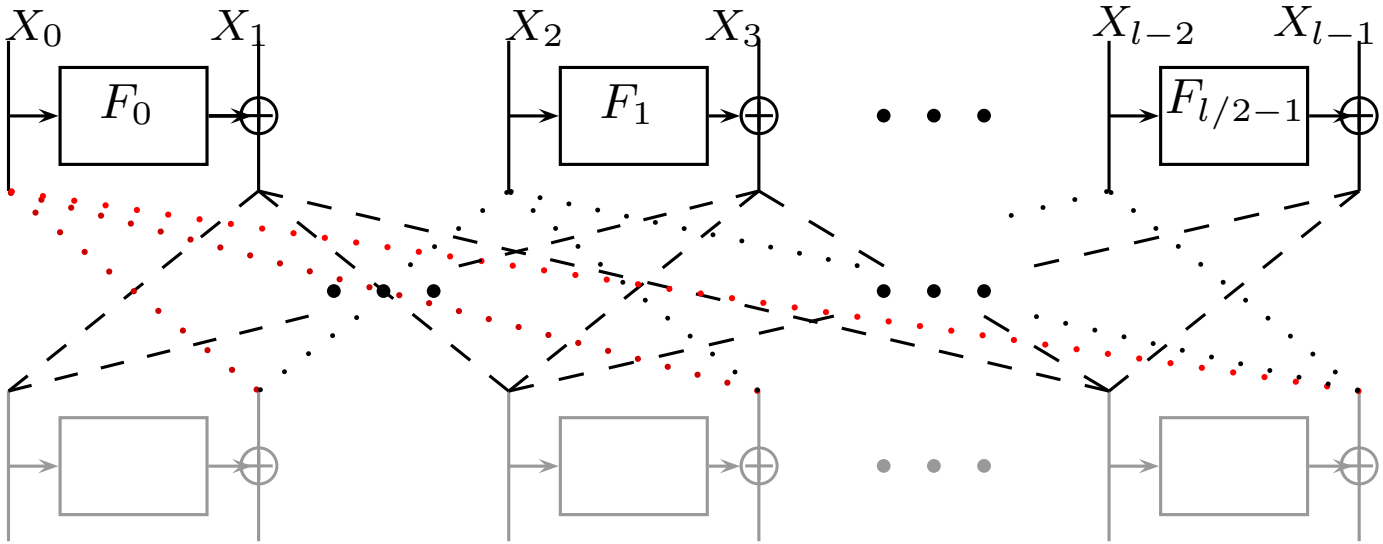


GFS Structures

- Relation

$$(X_0, X_1, ..., X_{l-1}) \rightarrow \pi(X_0, F_0(X_0) \oplus X_1, X_2, F_1(X_2) \oplus X_3, ..., F_{l/2-1}(X_{l-2}) \oplus X_{l-1})$$

- Figure

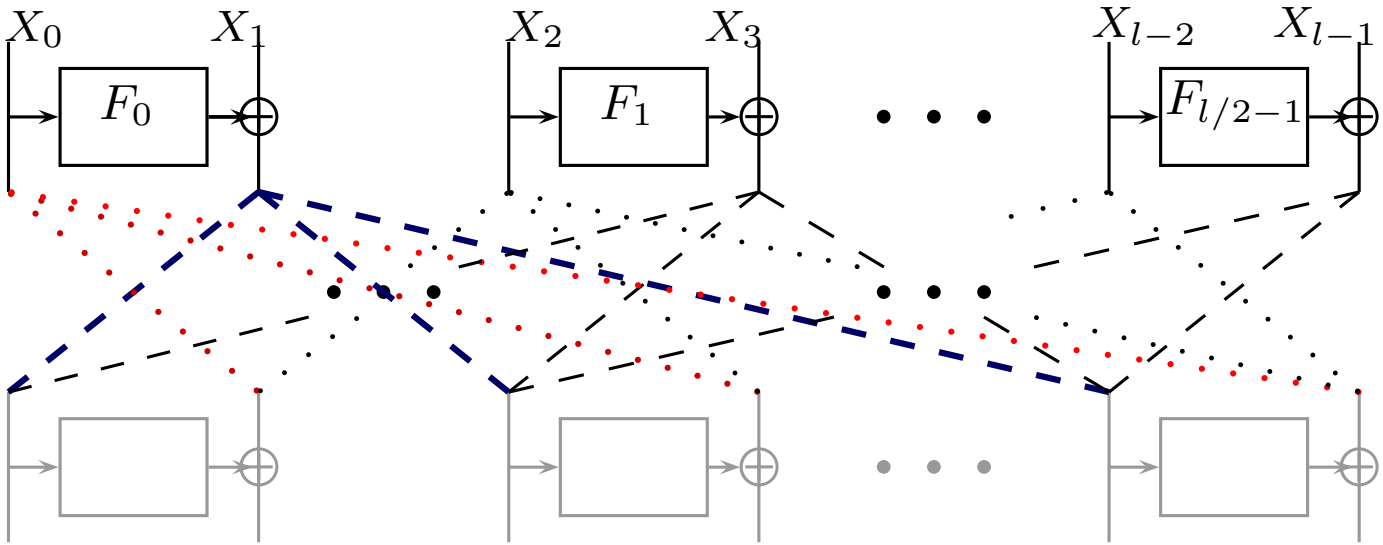


GFS Structures

- Relation

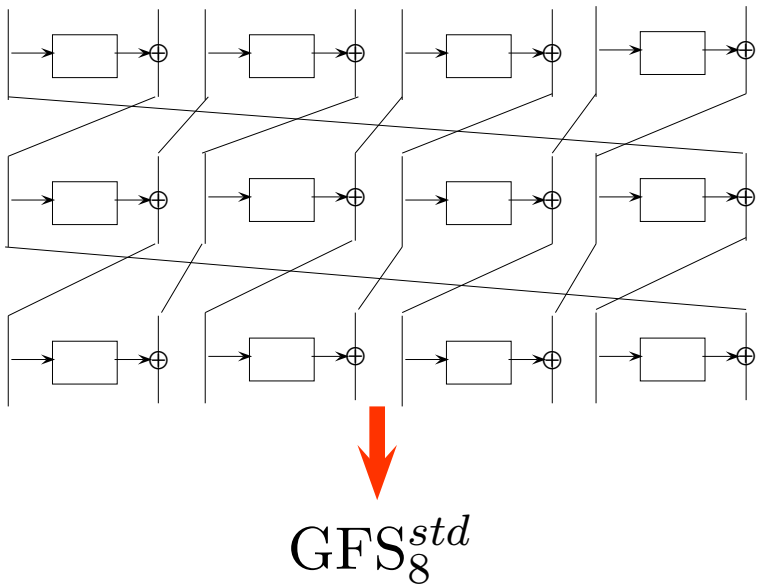
$$(X_0, X_1, ..., X_{l-1}) \rightarrow \pi(X_0, F_0(X_0) \oplus X_1, X_2, F_1(X_2) \oplus X_3, ..., F_{l/2-1}(X_{l-2}) \oplus X_{l-1})$$

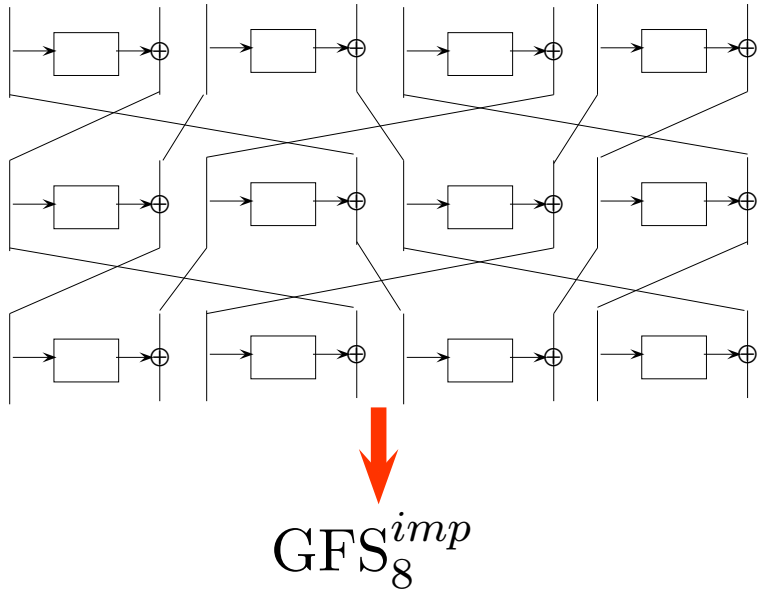
- Figure



GFS Structures

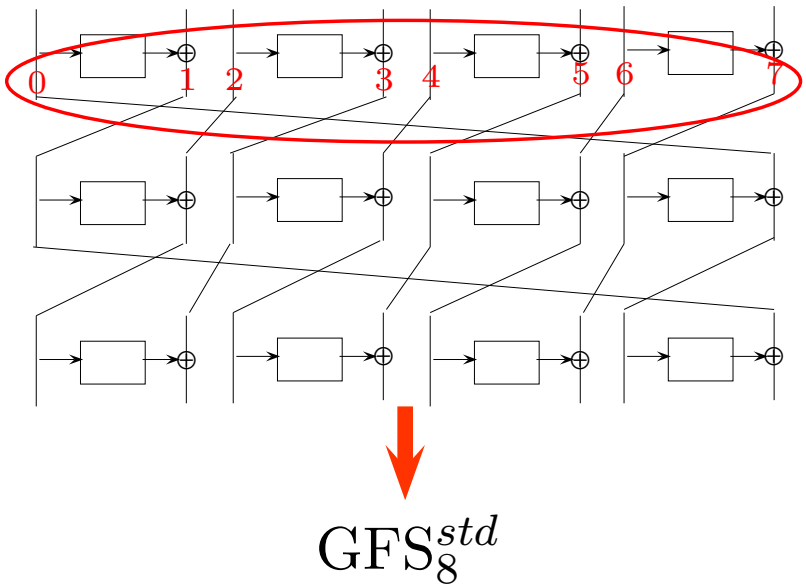
- Figures of GFS_8^{std} and GFS_8^{imp}





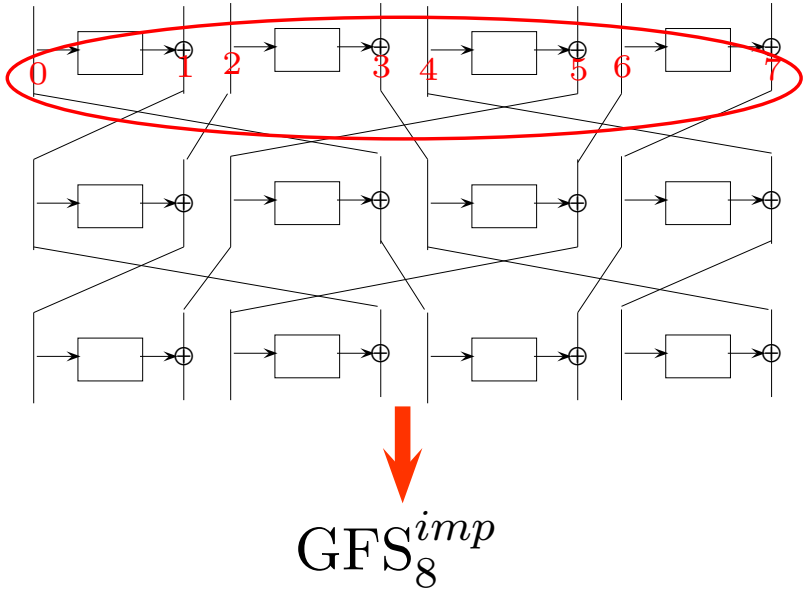
GFS Structures

- Figures of GFS_8^{std} and GFS_8^{imp}



GFS_8^{std}

$\pi(0, 1, ..., 7) = (7, 0, 1, 2, 3, 4, 5, 6)$



GFS_8^{imp}

$\pi(0, 1, ..., 7) = (3, 0, 1, 4, 7, 2, 5, 6)$

Table of Contents

Summation Representation

$$\begin{pmatrix} 6 \\ 15 \\ 0 \\ 158 \end{pmatrix}$$

Summation Representation

$$\begin{pmatrix} 6 \\ 15 \\ 0 \\ 158 \end{pmatrix} \xrightarrow{truncated}$$

Summation Representation

$$\begin{pmatrix} 6 \\ 15 \\ 0 \\ 158 \end{pmatrix} \xrightarrow{truncated} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

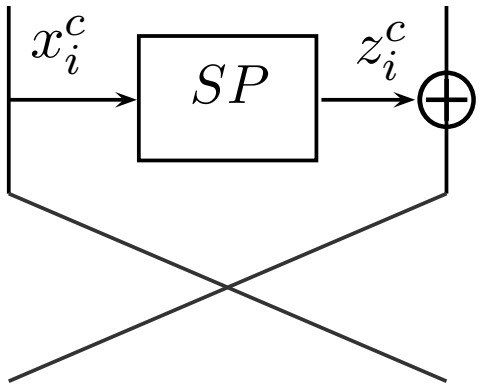
Summation Representation

$$\begin{pmatrix} 6 \\ 15 \\ 0 \\ 158 \end{pmatrix} \xrightarrow{truncated} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \xrightarrow{summation}$$

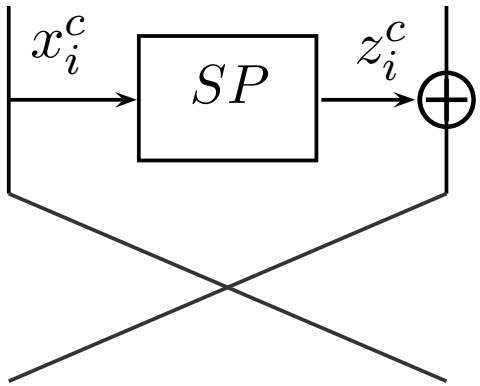
Summation Representation

$$\begin{pmatrix} 6 \\ 15 \\ 0 \\ 158 \end{pmatrix} \xrightarrow{truncated} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \xrightarrow{summation} 3$$

Equations Describing the SP-Function

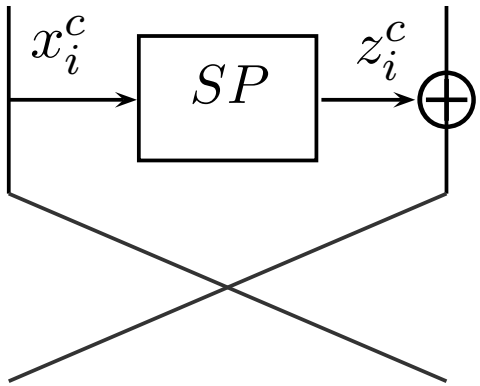


Equations Describing the SP-Function



The branch number of an $n \times n$ matrix P is $\beta = n + 1$, since P is an MDS matrix.

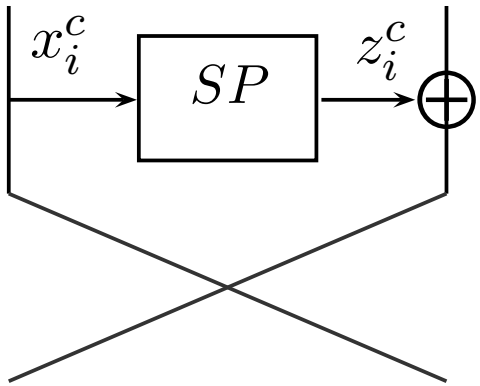
Equations Describing the SP-Function



The branch number of an $n \times n$ matrix P is $\beta = n + 1$, since P is an MDS matrix.

$$\begin{cases} z_i^c = 0 & \text{if } x_i^c = 0 \\ x_i^c + z_i^c \geq n + 1 & \text{otherwise} \end{cases}$$

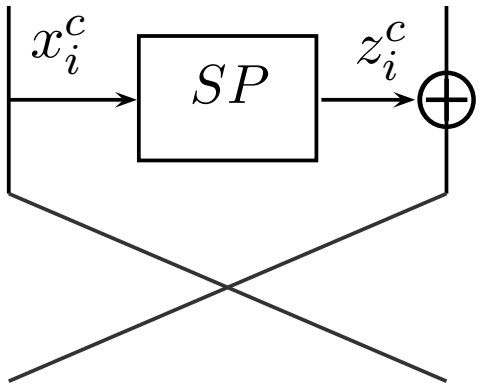
Equations Describing the SP-Function



The branch number of an $n \times n$ matrix P is $\beta = n + 1$, since P is an MDS matrix.

$$\begin{cases} z_i^c = 0 & \text{if } x_i^c = 0 \\ x_i^c + z_i^c \geq n + 1 & \text{otherwise} \end{cases} \qquad \begin{cases} x_i^c + z_i^c \geq n + 1 \\ 0 \leq x_i^c \leq n \\ 0 \leq z_i^c \leq n \end{cases}$$

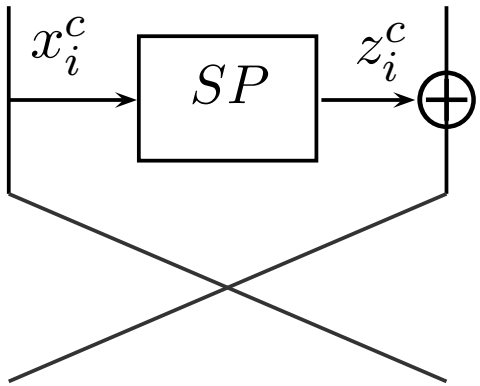
Equations Describing the SP-Function



The branch number of an $n \times n$ matrix P is $\beta = n + 1$, since P is an MDS matrix.

$$\begin{cases} z_i^c = 0 & \text{if } x_i^c = 0 \\ x_i^c + z_i^c \geq n + 1 & \text{otherwise} \end{cases} \qquad \begin{cases} x_i^c + z_i^c \geq n + 1 \\ 0 \leq x_i^c \leq n \\ 0 \leq z_i^c \leq n \end{cases}$$

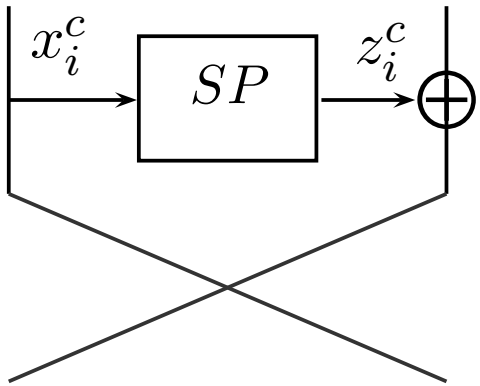
Equations Describing the SP-Function



The branch number of an $n \times n$ matrix P is $\beta = n + 1$, since P is an MDS matrix.

$$\begin{cases} z_i^c = 0 & \text{if } x_i^c = 0 \\ x_i^c + z_i^c \geq n + 1 & \text{otherwise} \end{cases} \qquad \begin{cases} x_i^c + z_i^c \geq (n+1)b_i \\ b_i \leq x_i^c \leq nb_i \\ b_i \leq z_i^c \leq nb_i \\ b_i \in \{0, 1\} \end{cases}$$

Equations Describing the SP-Function



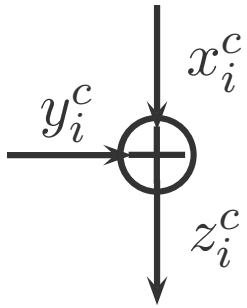
The branch number of an $n \times n$ matrix P is $\beta = n + 1$, since P is an MDS matrix.

$$\begin{cases} z_i^c = 0 & \text{if } x_i^c = 0 \\ x_i^c + z_i^c \geq n + 1 & \text{otherwise} \end{cases}$$

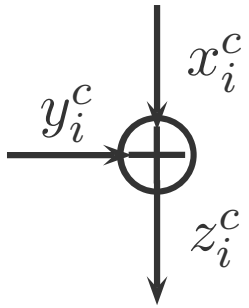
$$\begin{cases} x_i^c + z_i^c \geq (n+1)b_i \\ b_i \leq x_i^c \leq nb_i \\ b_i \leq z_i^c \leq nb_i \\ b_i \in \{0, 1\} \end{cases}$$

$$\begin{cases} 0 \leq x_i^c \leq n \\ 0 \leq z_i^c \leq n \\ x_i^c + z_i^c \geq (n+1)b_i \\ b_i \leq x_i^c \leq nb_i \\ z_i^c \leq nb_i \end{cases}$$

Equations Describing the XOR Operation

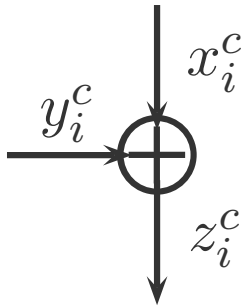


Equations Describing the XOR Operation



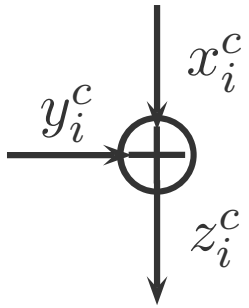
$$\begin{cases} x_i^c + z_i^c & \geq & y_i^c \\ \\ \|x_i^c - z_i^c\| & \leq & y_i^c \end{cases}$$

Equations Describing the XOR Operation



$$\begin{cases} x_i^c + z_i^c & \geq & y_i^c \\ \\ \|x_i^c - z_i^c\| & \leq & y_i^c \end{cases} \Longrightarrow$$

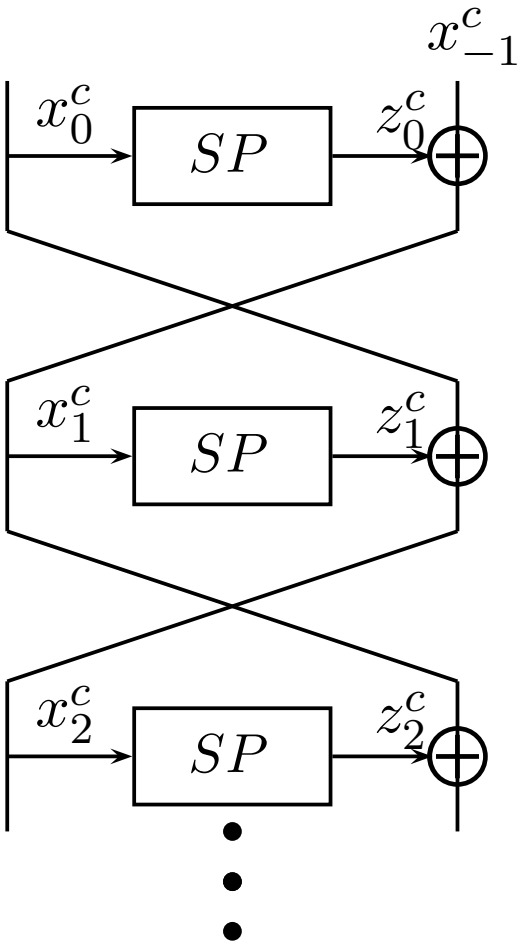
Equations Describing the XOR Operation



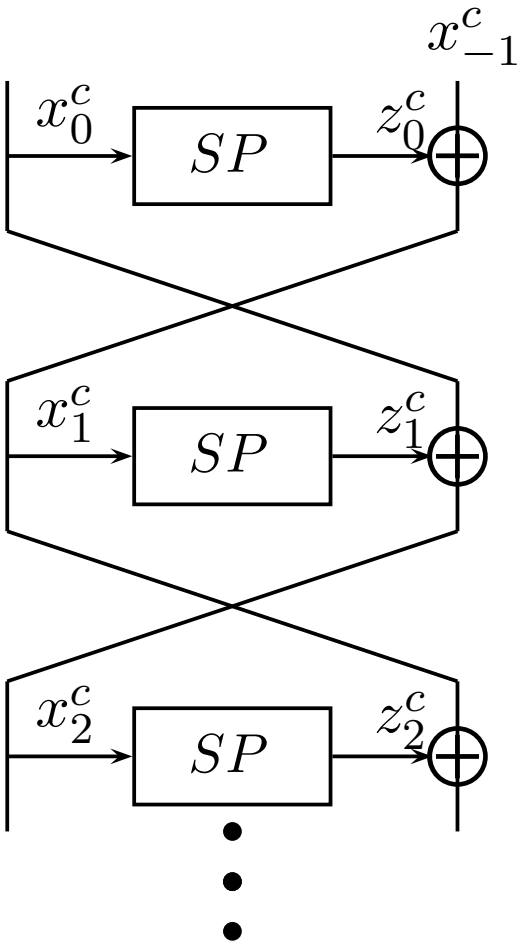
$$\begin{cases} x_i^c + z_i^c & \geq & y_i^c \\ \\ \|x_i^c - z_i^c\| & \leq & y_i^c \end{cases} \Longrightarrow \begin{cases} x_i^c + z_i^c \geq y_i^c \\ \\ x_i^c - z_i^c \leq y_i^c \\ \\ z_i^c - x_i^c \leq y_i^c \end{cases}$$

Table of Contents

Evaluating Two Sub-Blocks Feistel Structure

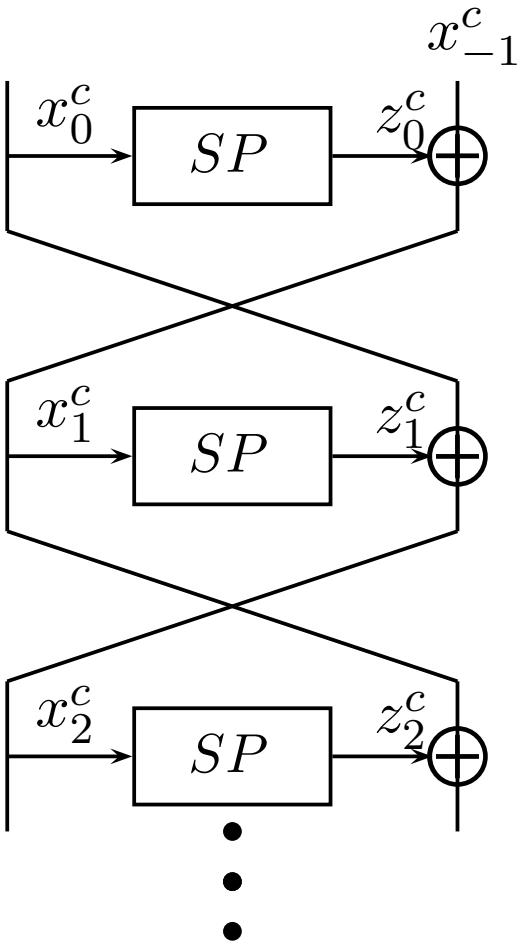


Evaluating Two Sub-Blocks Feistel Structure



$$\begin{cases} 0 \leq x_i^c \leq n \\ 0 \leq z_i^c \leq n \\ x_i^c + z_i^c \geq (n+1)b_i \\ b_i \leq x_i^c \leq nb_i \\ z_i^c \leq nb_i \end{cases}$$

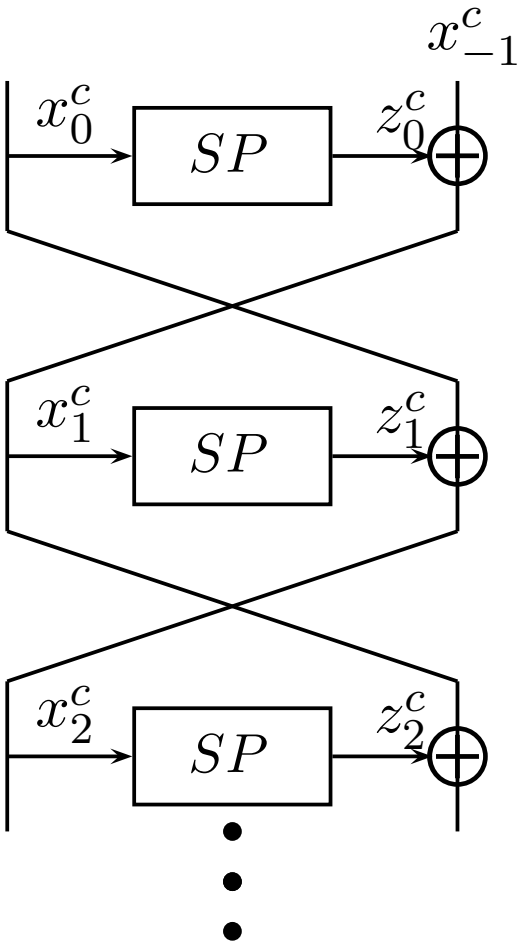
Evaluating Two Sub-Blocks Feistel Structure



$$\begin{cases} 0 \leq x_i^c \leq n \\ 0 \leq z_i^c \leq n \\ x_i^c + z_i^c \geq (n+1)b_i \\ b_i \leq x_i^c \leq nb_i \\ z_i^c \leq nb_i \end{cases}$$

$$\begin{cases} x_{i-2}^c + z_{i-1}^c \geq x_i^c \\ x_{i-2}^c - z_{i-1}^c \leq x_i^c \\ z_{i-1}^c - x_{i-2}^c \leq x_i^c \end{cases}$$

Evaluating Two Sub-Blocks Feistel Structure

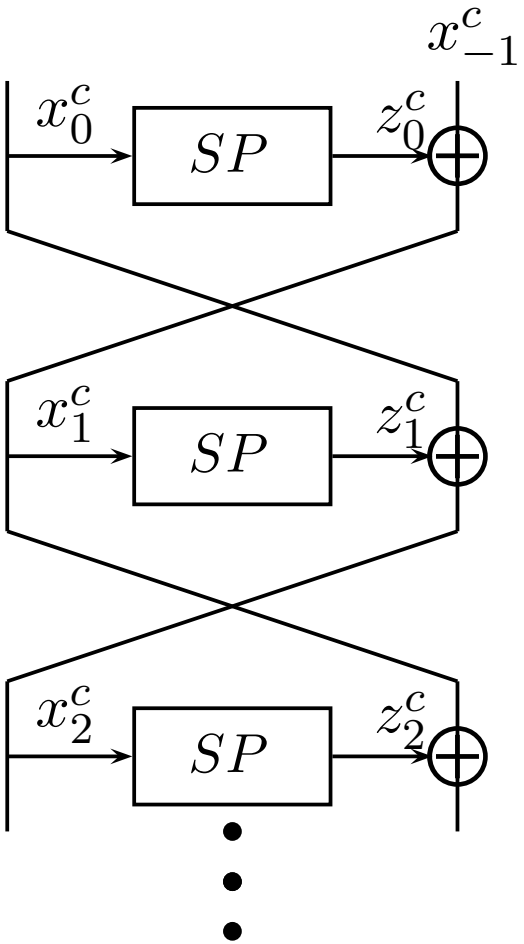


$$\begin{cases} 0 \leq x_i^c \leq n \\ 0 \leq z_i^c \leq n \\ x_i^c + z_i^c \geq (n+1)b_i \\ b_i \leq x_i^c \leq nb_i \\ z_i^c \leq nb_i \end{cases}$$

$$\begin{cases} x_{i-2}^c + z_{i-1}^c \geq x_i^c \\ x_{i-2}^c - z_{i-1}^c \leq x_i^c \\ z_{i-1}^c - x_{i-2}^c \leq x_i^c \end{cases}$$

$$x_{-1}^c + x_0^c \geq 1$$

Evaluating Two Sub-Blocks Feistel Structure



$$\begin{cases} 0 \leq x_i^c \leq n \\ 0 \leq z_i^c \leq n \\ x_i^c + z_i^c \geq (n+1)b_i \\ b_i \leq x_i^c \leq nb_i \\ z_i^c \leq nb_i \end{cases}$$

$$\begin{cases} x_{i-2}^c + z_{i-1}^c \geq x_i^c \\ x_{i-2}^c - z_{i-1}^c \leq x_i^c \\ z_{i-1}^c - x_{i-2}^c \leq x_i^c \end{cases}$$

$$x_{-1}^c + x_0^c \geq 1$$

Objective function: $min(\sum_{j=0}^{n-1} x_j^c)$

Evaluating Two Sub-Blocks Feistel Structure

- **Table 1.** Minimum number of active S-boxes of two sub-blocks Feistel

Round	Feistel $(n = 4)$	Feistel $(n = 8)$
1	0	0
2	1	1
3	2	2
4	5	9
5	6	10
6	7	11
7	8	12
8	11	19
9	12	20
10	13	21
11	14	22
12	17	29
13	18	30
14	19	31
15	20	32
16	23	39
17	24	40
18	25	41

Table of Contents

Evaluating Generalized Feistel Structures

- **Table 2.** The Minimum Number of Active S-boxes in GFS_l^{std} with $n = 4$

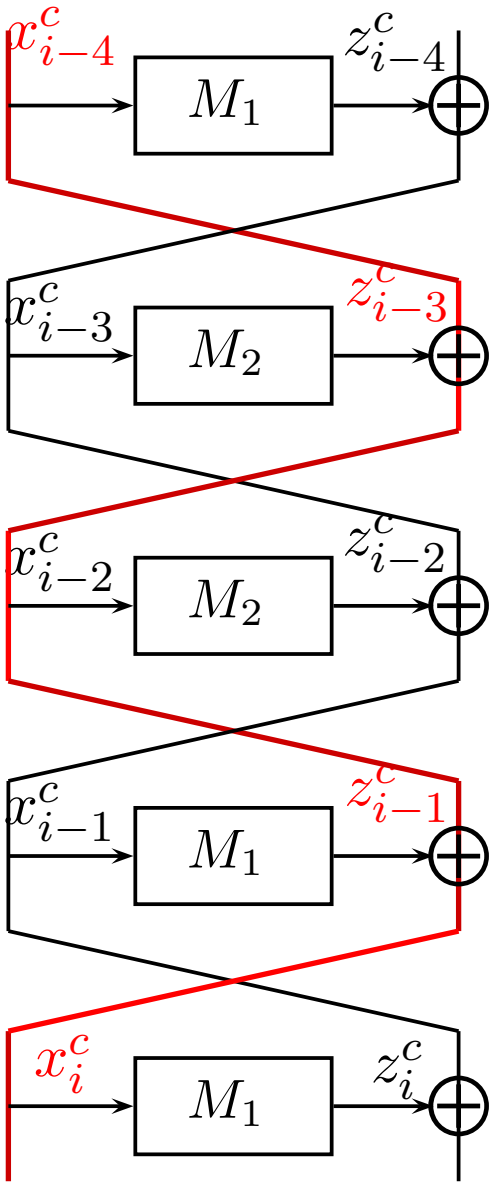
	$l=4$		$l=6$		$l=8$		$l=10$		$l=12$		$l=14$		$l=16$	
Round	*	[1]	*	[1]	*	[1]	*	[1]	*	[1]	*	[1]	*	[1]
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	2	2	2	2	2	2	2	2	2	2	2	2	2	2
4	6	6	6	6	6	6	6	6	6	6	6	6	6	6
5	8	8	8	8	8	8	8	8	8	8	8	8	8	8
6	12	12	12	12	12	12	12	12	12	12	12	12	12	12
7	12	12	14	14	14	14	14	14	14	14	14	14	14	14
8	13	13	18	18	18	18	18	18	18	18	18	18	18	18
9	14	14	21	21	21	21	21	21	21	21	21	21	21	21
10	18	18	25	25	25	25	25	25	25	25	25	25	25	25
11	20	20	27	27	28	28	28	28	28	28	28	28	28	28
12	24	24	30	30	36	36	36	36	36	36	36	36	36	36
13	24	24	31	31	36	36	39	39	39	39	39	39	39	39
14	25	25	35	35	37	37	43	43	43	43	43	43	43	43
15	26	26	37	37	38	38	47	47	47	47	47	47	47	47
16	30	30	41	41	42	42	54	54	54	54	54	54	54	54
17	32	32	43	43	44	44	58	58	58	58	58	58	52	52
18	36	36	47	47	48	48	**62**	58	62	62	62	62	62	62

Evaluating Generalized Feistel Structures

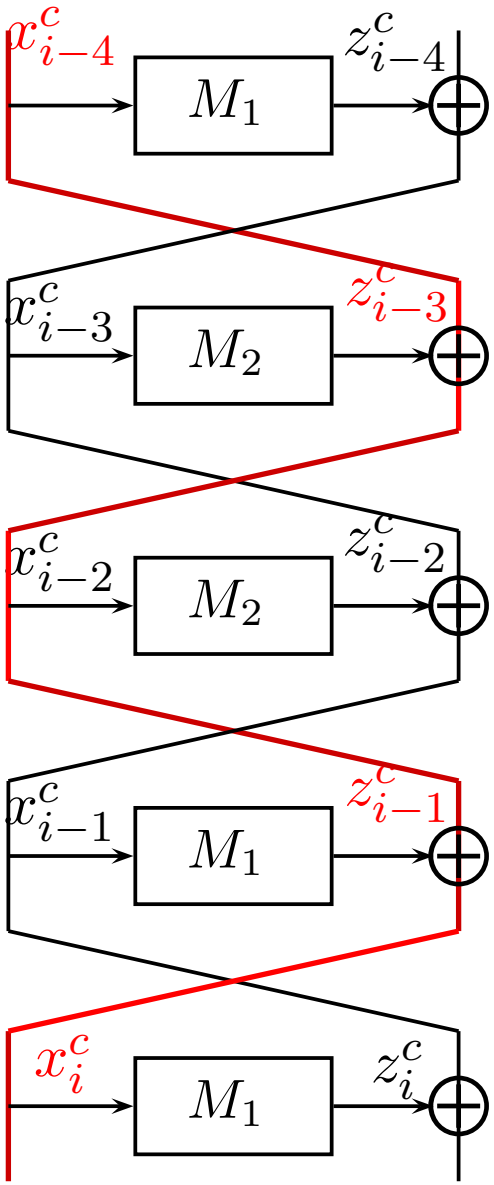
- **Table 3.** The Minimum Number of Active S-boxes in GFS_l^{imp} with $n = 4$

	$l = 6$		$l = 8$		$l = 10$		$l = 12$		$l = 14$		$l = 16$	
Round	*	[1]	*	[1]	*	[1]	*	[1]	*	[1]	*	[1]
1	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1
3	2	2	2	2	2	2	2	2	2	2	2	2
4	6	6	6	6	6	6	6	6	6	6	6	6
5	8	8	8	8	8	8	8	8	8	8	8	8
6	12	12	12	12	12	12	12	12	12	12	12	12
7	14	14	14	14	14	14	14	14	14	14	14	14
8	**23**	22	23	23	**26**	23	18	18	**26**	23	**26**	23
9	24	24	26	26	29	29	21	21	29	29	31	31
10	26	26	29	29	**35**	34	29	29	37	37	**43**	40
11	28	28	32	32	36	36	32	32	40	40	48	48
12	32	32	39	39	**43**	45	**42**	39	**52**	49	**57**	54
13	**34**	33	**42**	40	44	44	45	45	54	54	60	60
14	38	38	**45**	44	48	48	**54**	53	**64**	60	**66**	63
15	40	40	46	46	50	50	57	57	**66**	63	**69**	70
16	**48**	46	50	50	54	54	**61**	60	**77**	71	76	76
17	48	48	52	52	56	56	64	64	**82**	76	78	78
18	50	50	56	56	**68**	65	**70**	68	**84**	83	87	87

Evaluating Switching Mechanism

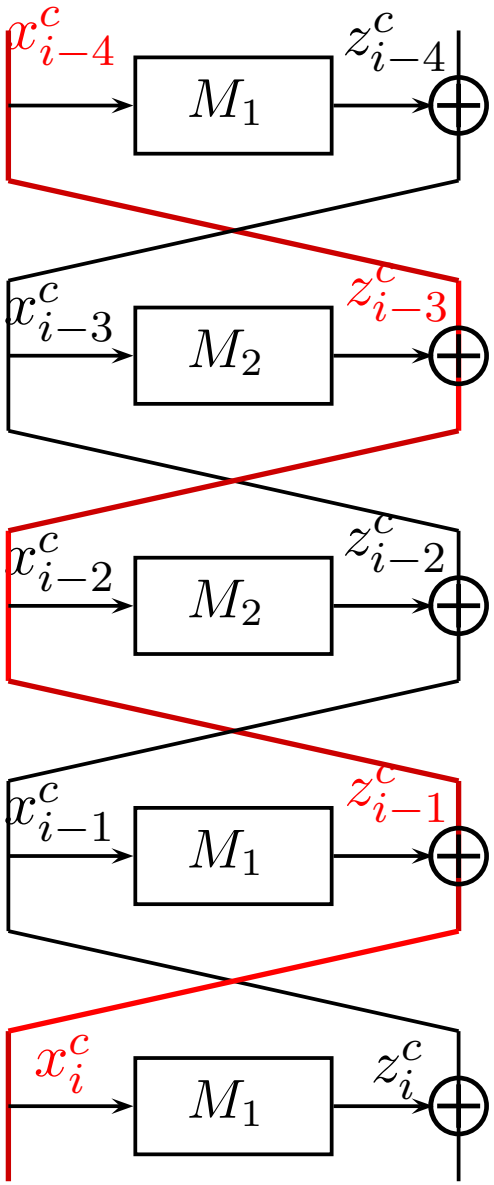


Evaluating Switching Mechanism



$$\mathbf{x_i} = \mathbf{z_{i-1}} \oplus \mathbf{z_{i-3}} \oplus \mathbf{x_{i-4}}$$

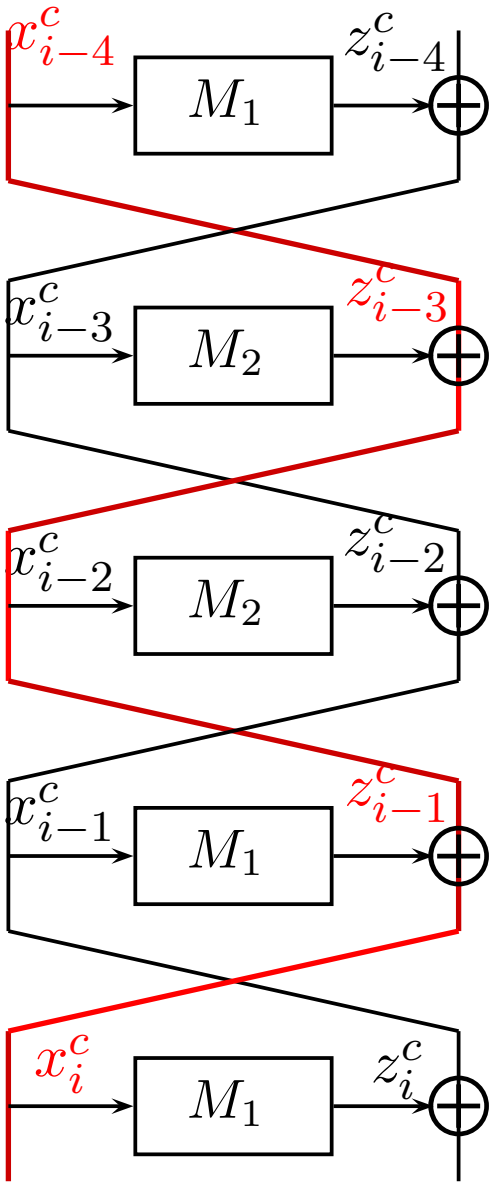
Evaluating Switching Mechanism



$$\mathbf{x_i} = \mathbf{z_{i-1}} \oplus \mathbf{z_{i-3}} \oplus \mathbf{x_{i-4}}$$

$$\begin{bmatrix} \mathbf{M_1} & \mathbf{M_2} \end{bmatrix} \begin{bmatrix} \mathbf{x_{i-1}} \\ \mathbf{x_{i-3}} \end{bmatrix} = \mathbf{x_i} \oplus \mathbf{x_{i-4}}$$

Evaluating Switching Mechanism

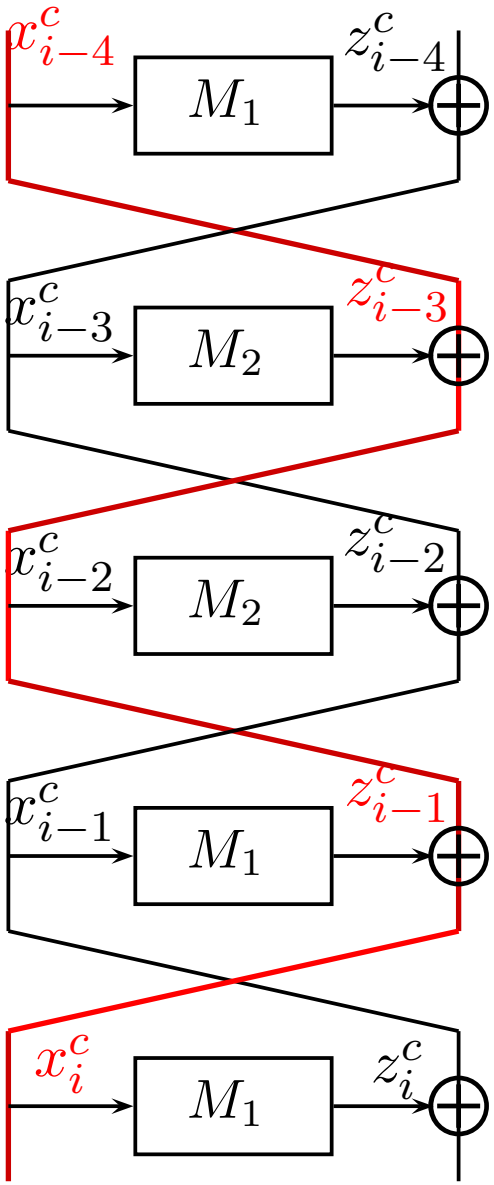


$$\mathbf{x_i} = \mathbf{z_{i-1}} \oplus \mathbf{z_{i-3}} \oplus \mathbf{x_{i-4}}$$

$$\begin{bmatrix} \mathbf{M_1} & \mathbf{M_2} \end{bmatrix} \begin{bmatrix} \mathbf{x_{i-1}} \\ \mathbf{x_{i-3}} \end{bmatrix} = \mathbf{x_i} \oplus \mathbf{x_{i-4}}$$

$$x^c_i + x^c_{i-1} + x^c_{i-3} + x^c_{i-4} \geq (n+1)$$

Evaluating Switching Mechanism



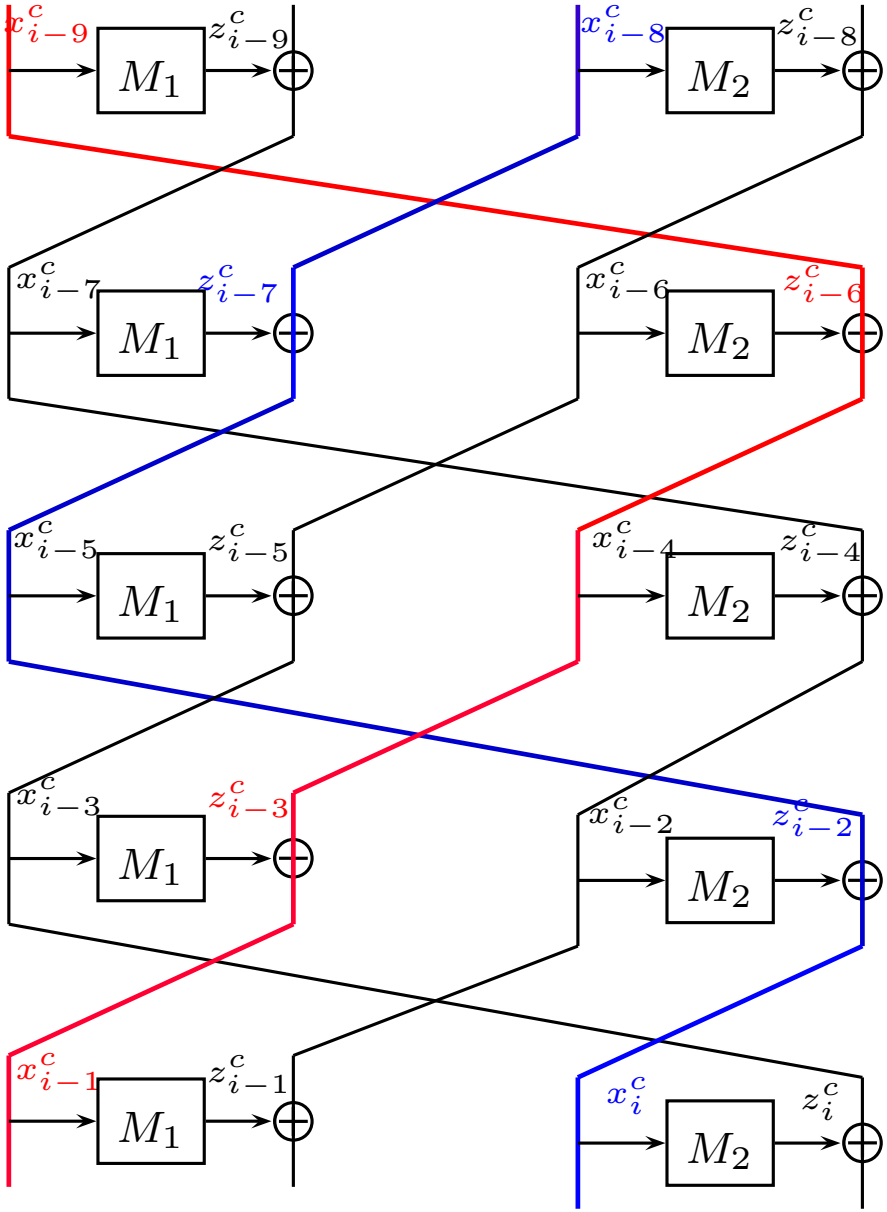
$$\mathbf{x_i} = \mathbf{z_{i-1}} \oplus \mathbf{z_{i-3}} \oplus \mathbf{x_{i-4}}$$

$$\begin{bmatrix} \mathbf{M_1} & \mathbf{M_2} \end{bmatrix} \begin{bmatrix} \mathbf{x_{i-1}} \\ \mathbf{x_{i-3}} \end{bmatrix} = \mathbf{x_i} \oplus \mathbf{x_{i-4}}$$

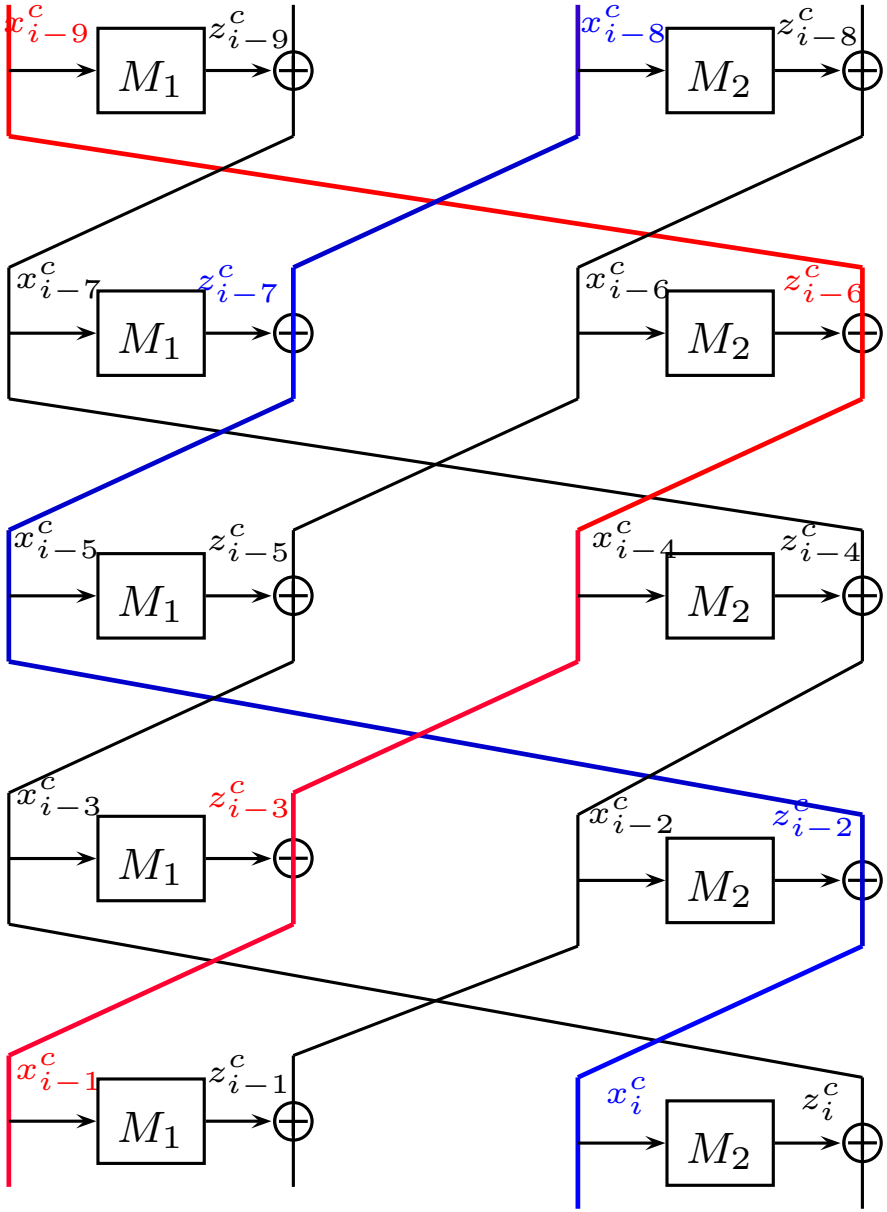
$$x^c_i + x^c_{i-1} + x^c_{i-3} + x^c_{i-4} \geq (n+1)$$

$$\begin{cases} x^c_i + x^c_{i-1} + x^c_{i-3} + x^c_{i-4} \geq (n+1)bb_i \\ bb_i \leq x^c_{i-1} + x^c_{i-3} \leq 2nbb_i \end{cases}$$

Evaluating Switching Mechanism

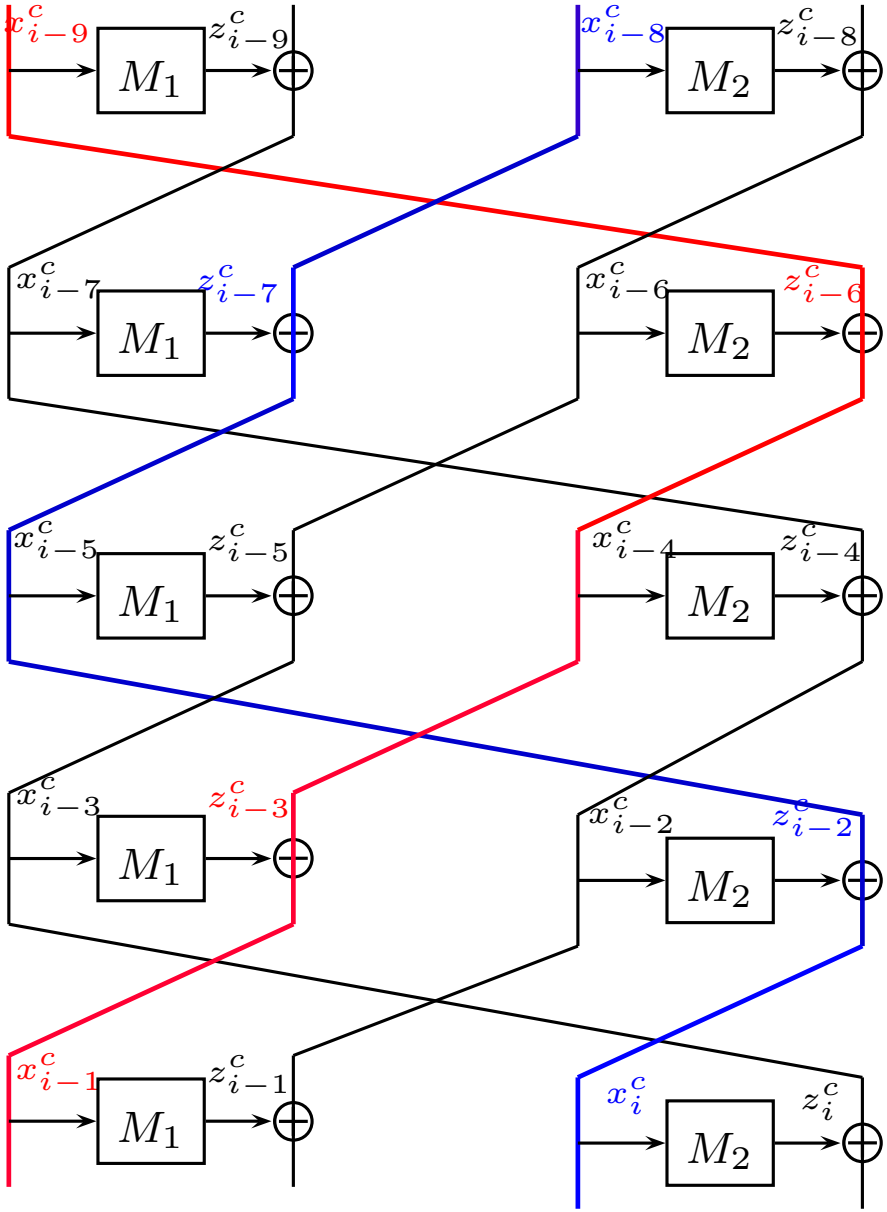


Evaluating Switching Mechanism



$$\mathbf{x_{i-1}} = \mathbf{z_{i-3}} \oplus \mathbf{z_{i-6}} \oplus \mathbf{x_{i-9}}$$

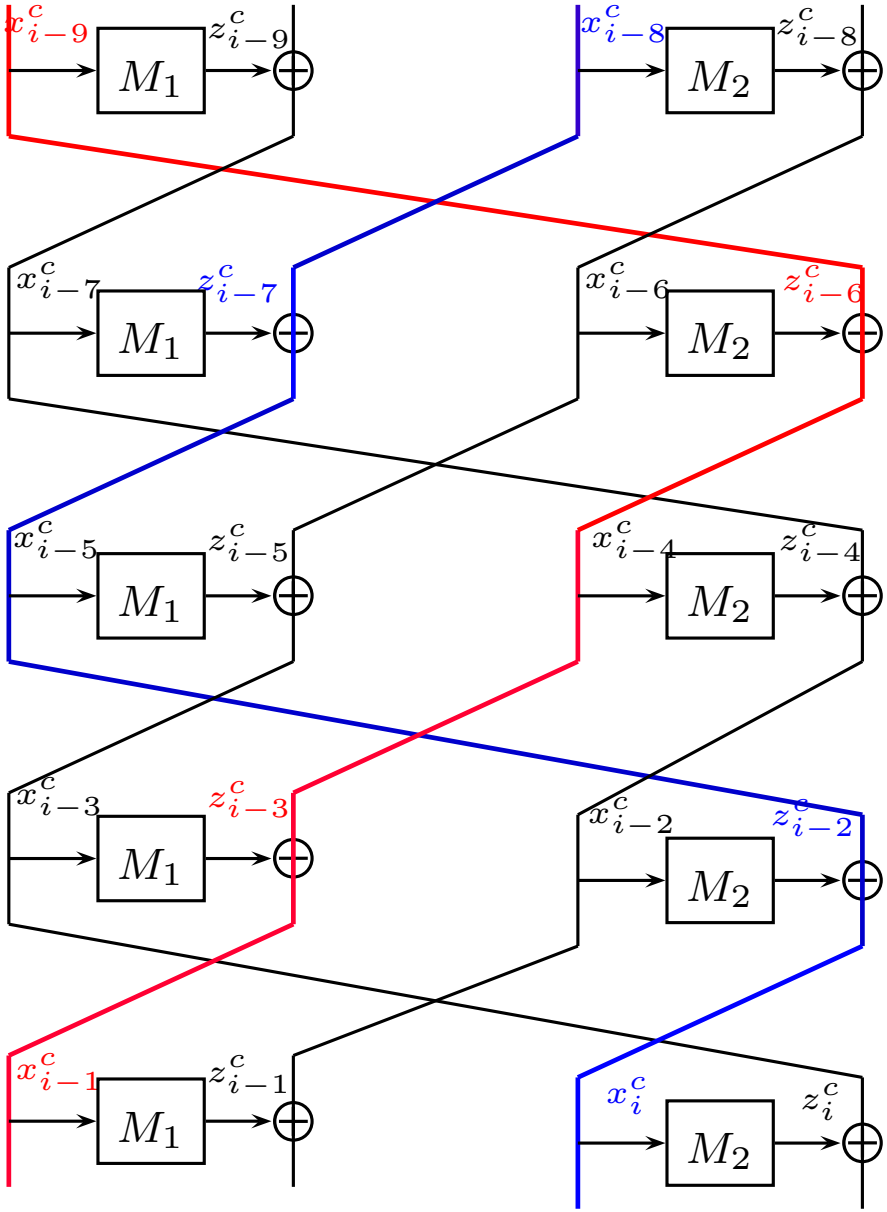
Evaluating Switching Mechanism



$$\mathbf{x_{i-1} = z_{i-3} \oplus z_{i-6} \oplus x_{i-9}}$$

$$\begin{cases} x^c_{i-1} + x^c_{i-3} + x^c_{i-6} + x^c_{i-9} \geq (n+1)bb_{i-1} \\ bb_{i-1} \leq x^c_{i-3} + x^c_{i-6} \leq 2nbb_{i-1} \end{cases}$$

Evaluating Switching Mechanism

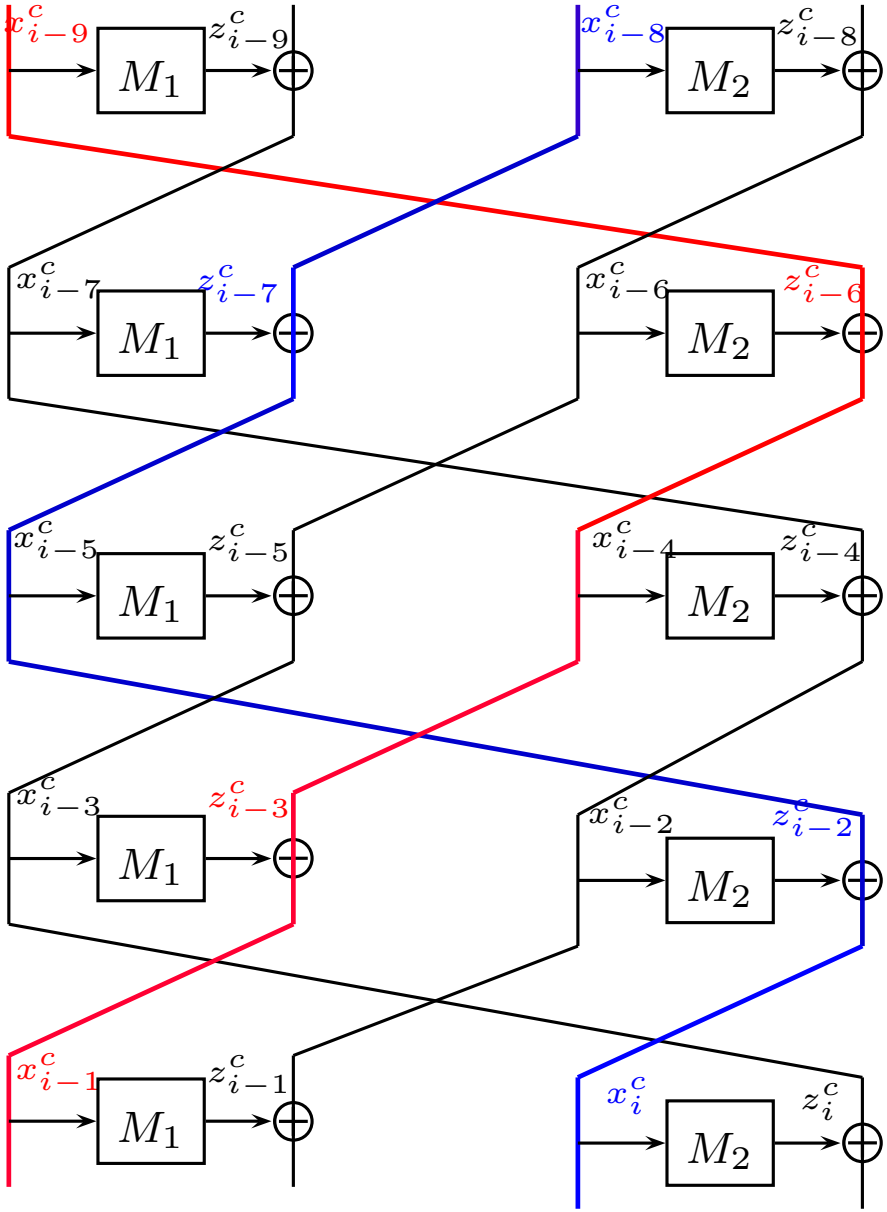


$$\mathbf{x_{i-1} = z_{i-3} \oplus z_{i-6} \oplus x_{i-9}}$$

$$\begin{cases} x^c_{i-1} + x^c_{i-3} + x^c_{i-6} + x^c_{i-9} \geq (n+1)bb_{i-1} \\ bb_{i-1} \leq x^c_{i-3} + x^c_{i-6} \leq 2nbb_{i-1} \end{cases}$$

$$\mathbf{x_i = z_{i-2} \oplus z_{i-7} \oplus x_{i-8}}$$

Evaluating Switching Mechanism



$$\mathbf{x_{i-1} = z_{i-3} \oplus z_{i-6} \oplus x_{i-9}}$$

$$\begin{cases} x^c_{i-1} + x^c_{i-3} + x^c_{i-6} + x^c_{i-9} \geq (n+1)bb_{i-1} \\ bb_{i-1} \leq x^c_{i-3} + x^c_{i-6} \leq 2nbb_{i-1} \end{cases}$$

$$\mathbf{x_i = z_{i-2} \oplus z_{i-7} \oplus x_{i-8}}$$

$$\begin{cases} x^c_i + x^c_{i-2} + x^c_{i-7} + x^c_{i-8} \geq (n+1)bb_i \\ bb_i \leq x^c_{i-2} + x^c_{i-7} \leq 2nbb_i \end{cases}$$

Evaluating Switching Mechanism

- GFS_6^{std}

Evaluating Switching Mechanism

- GFS_6^{std}

$$\mathbf{x_{i-2}} = \mathbf{z_{i-5}} \oplus \mathbf{z_{i-9}} \oplus \mathbf{z_{i-16}} \oplus \mathbf{x_{i-20}}$$

Evaluating Switching Mechanism

- GFS_6^{std}

$$\mathbf{x_{i-2}} = \mathbf{z_{i-5}} \oplus \mathbf{z_{i-9}} \oplus \mathbf{z_{i-16}} \oplus \mathbf{x_{i-20}}$$

$$\begin{cases} x^c_{i-2} + x^c_{i-5} + x^c_{i-9} + x^c_{i-16} + x^c_{i-20} \geq (n+1)bb_{i-2} \\ bb_{i-2} \leq x^c_{i-5} + x^c_{i-9} + x^c_{i-16} \leq 3nbb_{i-2} \end{cases}$$

Evaluating Switching Mechanism

- GFS_6^{std}

$$\mathbf{x_{i-2}} = \mathbf{z_{i-5}} \oplus \mathbf{z_{i-9}} \oplus \mathbf{z_{i-16}} \oplus \mathbf{x_{i-20}}$$

$$\begin{cases} x^c_{i-2} + x^c_{i-5} + x^c_{i-9} + x^c_{i-16} + x^c_{i-20} \geq (n+1)bb_{i-2} \\ bb_{i-2} \leq x^c_{i-5} + x^c_{i-9} + x^c_{i-16} \leq 3nbb_{i-2} \end{cases}$$

- GFS_8^{imp}

Evaluating Switching Mechanism

- GFS_6^{std}

$$\mathbf{x_{i-2}} = \mathbf{z_{i-5}} \oplus \mathbf{z_{i-9}} \oplus \mathbf{z_{i-16}} \oplus \mathbf{x_{i-20}}$$

$$\begin{cases} x^c_{i-2} + x^c_{i-5} + x^c_{i-9} + x^c_{i-16} + x^c_{i-20} \geq (n+1)bb_{i-2} \\ bb_{i-2} \leq x^c_{i-5} + x^c_{i-9} + x^c_{i-16} \leq 3nbb_{i-2} \end{cases}$$

- GFS_8^{imp}

$$\mathbf{x_{i-3}} = \mathbf{z_{i-7}} \oplus \mathbf{z_{i-13}} \oplus \mathbf{z_{i-20}} \oplus \mathbf{x_{i-30}} \oplus \mathbf{x_{i-35}}$$

Evaluating Switching Mechanism

- GFS_6^{std}

$$\mathbf{x_{i-2}} = \mathbf{z_{i-5}} \oplus \mathbf{z_{i-9}} \oplus \mathbf{z_{i-16}} \oplus \mathbf{x_{i-20}}$$

$$\begin{cases} x^c_{i-2} + x^c_{i-5} + x^c_{i-9} + x^c_{i-16} + x^c_{i-20} \geq (n+1)bb_{i-2} \\ bb_{i-2} \leq x^c_{i-5} + x^c_{i-9} + x^c_{i-16} \leq 3nbb_{i-2} \end{cases}$$

- GFS_8^{imp}

$$\mathbf{x_{i-3}} = \mathbf{z_{i-7}} \oplus \mathbf{z_{i-13}} \oplus \mathbf{z_{i-20}} \oplus \mathbf{x_{i-30}} \oplus \mathbf{x_{i-35}}$$

$$\begin{cases} x^c_{i-3} + x^c_{i-7} + x^c_{i-13} + x^c_{i-20} + x^c_{i-30} + x^c_{i-35} \geq (n+1)bb_{i-3} \\ bb_{i-3} \leq x^c_{i-7} + x^c_{i-13} + x^c_{i-20} + x^c_{i-30} \leq 4nbb_{i-3} \end{cases}$$

Evaluating Switching Mechanism

- **Table 3.** Minimum number of differentially active S-boxes of generalized Feistel structures imposed by switching properties with n=4

Evaluating Switching Mechanism

- **Table 3.** Minimum number of differentially active S-boxes of generalized Feistel structures imposed by switching properties with n=4

	2 MDS matrices			3 MDS matrices			4 MDS matrices		5 MDS matrices		6 MDS matrices	
Round	Feistel	CLEFIA	GFS_8^{imp}	GFS_6^{std}	GFS_6^{imp}	GFS_{12}^{imp}	GFS_8^{std}	GFS_8^{imp}	GFS_{10}^{std}	GFS_{10}^{imp}	GFS_{12}^{std}	GFS_{12}^{imp}
1	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1	1	1
3	2	2	2	2	2	2	2	2	2	2	2	2
4	5	6	6	6	6	6	6	6	6	6	6	6
5	6	8	8	8	8	8	8	8	8	8	8	8
6	10	12	12	12	12	12	12	12	12	12	12	12
7	10	14	14	14	14	14	14	14	14	14	14	14
8	11	18	26	18	25	26	18	23	18	26	18	26
9	12	20	29	21	27	29	21	26	21	29	21	29
10	15	22	34	25	31	41	26	32	25	37	25	37
11	16	24	37	28	33	44	31	36	28	40	28	42
12	20	28	42	34	36	56	36	44	36	49	36	50
13	20	30	43	37	38	61	41	46	39	51	39	54
14	21	34	47	38	43	67	48	49	47	54	45	65
15	22	36	49	42	46	69	50	52	51	56	50	72
16	25	38	53	44	52	72	53	56	58	62	56	77
17	26	40	55	48	55	75	56	60	64	66	62	79
18	30	44	64	50	59	79	59	67	68	70	67	85
19	30	46	67	54	61	81	62	69	72	78	75	88
20	31	50	72	57	64	92	66	77	74	83	85	..
21	32	52	74	61	67	..	69	80	78	88	88	..
22	35	55	83	64	72	..	73	86	80	95	92	..
23	36	56	84	69	76	..	76	88	84	97	94	..
24	40	59	88	73	81	..	80	91	87	..	..	..

Counting the Linearly Active S-boxes

- Transforming differential vectors to linear masks

Counting the Linearly Active S-boxes

- Transforming differential vectors to linear masks

  - In linear cryptanalysis, Feistel structures with SP-functions converts to Feistel structures with PS-functions [2].

Counting the Linearly Active S-boxes

- Transforming differential vectors to linear masks

  - In linear cryptanalysis, Feistel structures with SP-functions converts to Feistel structures with PS-functions [2].

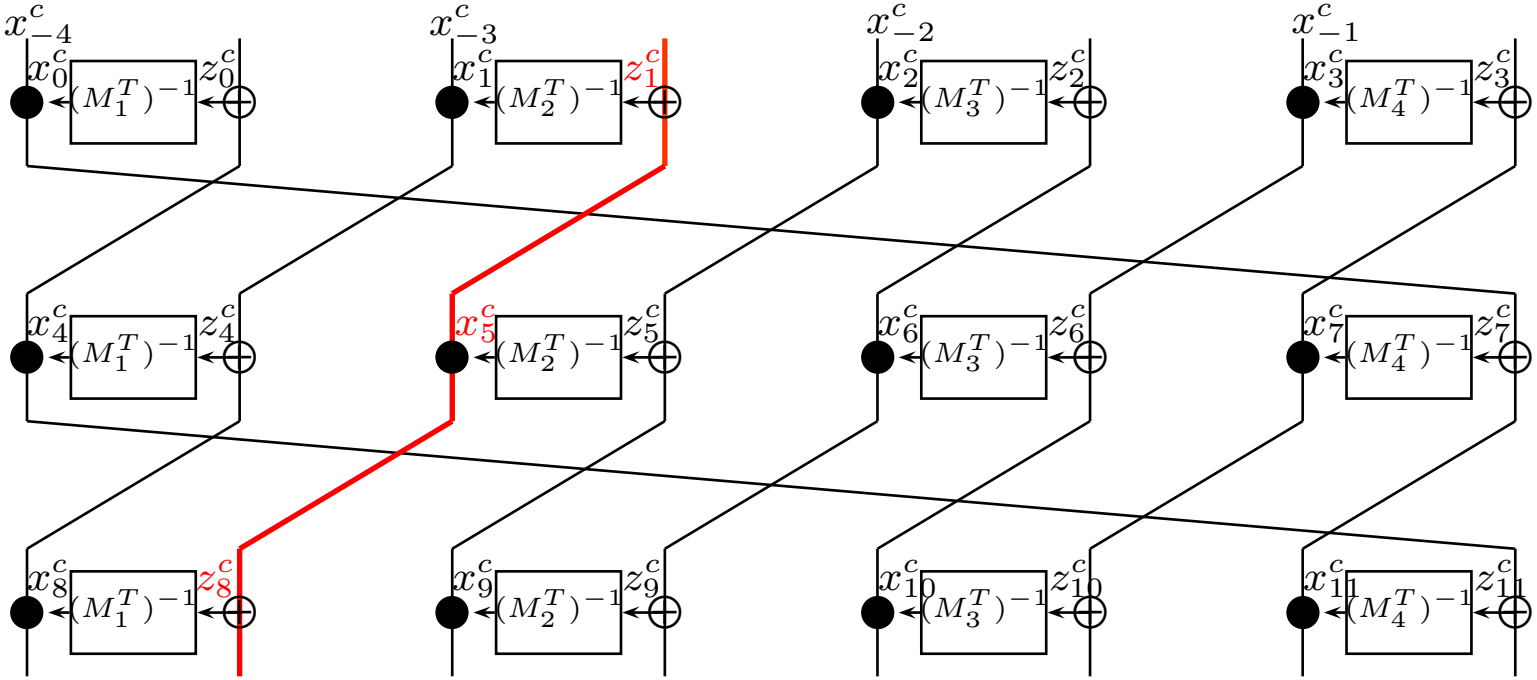
    - $\mathbf{x}^c$ denotes the summation representation of vector $\mathbf{\Gamma}.\mathbf{x}$.

Counting the Linearly Active S-boxes

- Defining summation variables of GFS_8^{std} in linear cryptanalysis

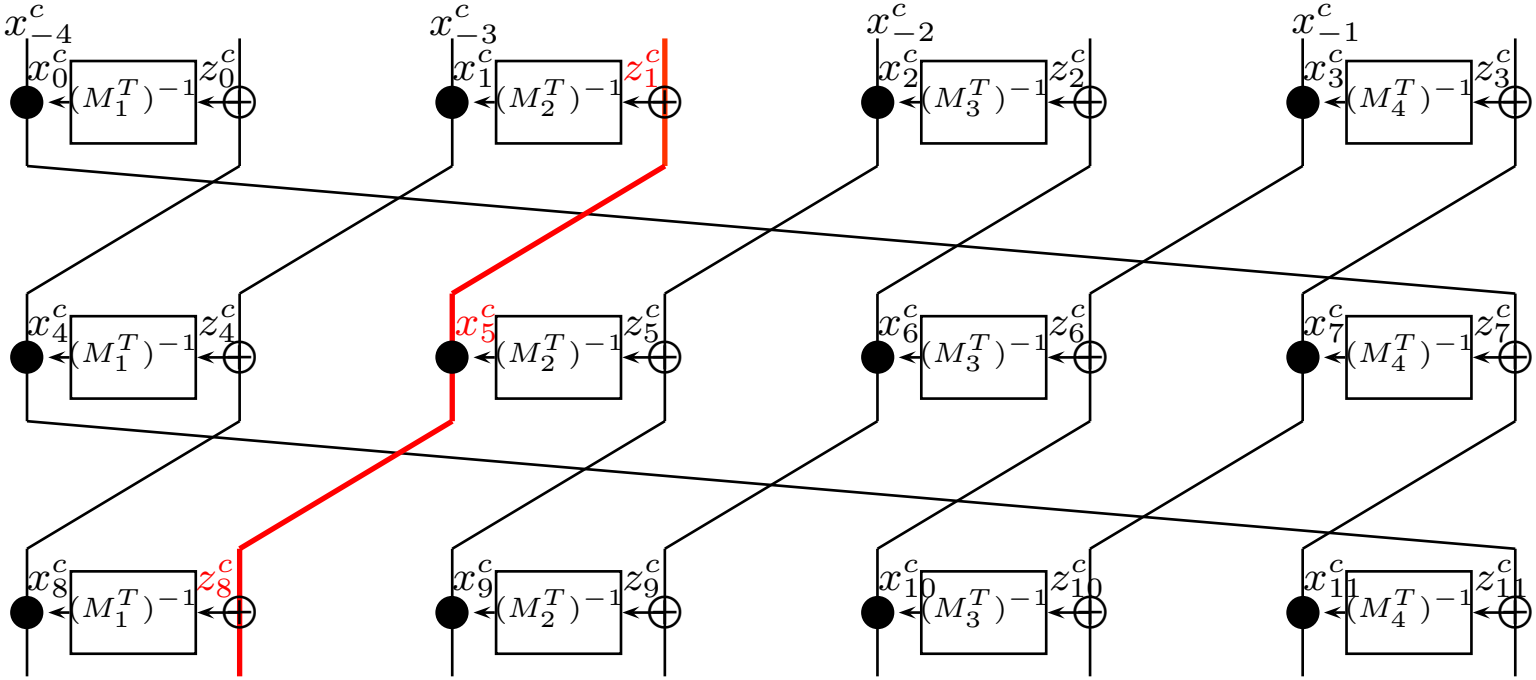
Counting the Linearly Active S-boxes

- Defining summation variables of GFS_8^{std} in linear cryptanalysis



Counting the Linearly Active S-boxes

- Defining summation variables of GFS_8^{std} in linear cryptanalysis



$$\mathbf{\Gamma.x_5 = \Gamma.x_1 \bullet \Gamma.x_8}$$

Counting the Linearly Active S-boxes

- One of the relations between inputs and outputs of three consecutive rounds

Counting the Linearly Active S-boxes

- One of the relations between inputs and outputs of three consecutive rounds

$$\mathbf{\Gamma.x_5} = \begin{bmatrix} (\mathbf{M_1^T})^{-1} & (\mathbf{M_2^T})^{-1} \end{bmatrix} \begin{bmatrix} \mathbf{\Gamma.x_1} \\ \mathbf{\Gamma.x_8} \end{bmatrix}$$

Counting the Linearly Active S-boxes

- One of the relations between inputs and outputs of three consecutive rounds

$$\mathbf{\Gamma}.\mathbf{x_5} = \begin{bmatrix} (\mathbf{M_1^T})^{-1} & (\mathbf{M_2^T})^{-1} \end{bmatrix} \begin{bmatrix} \mathbf{\Gamma}.\mathbf{x_1} \\ \mathbf{\Gamma}.\mathbf{x_8} \end{bmatrix}$$

- One of amounts $\mathbf{x_1}$ and $\mathbf{x_8}$ must be nonzero

Counting the Linearly Active S-boxes

- One of the relations between inputs and outputs of three consecutive rounds

$$\mathbf{\Gamma.x_5} = \begin{bmatrix} (\mathbf{M_1^T})^{-1} & (\mathbf{M_2^T})^{-1} \end{bmatrix} \begin{bmatrix} \mathbf{\Gamma.x_1} \\ \mathbf{\Gamma.x_8} \end{bmatrix}$$

- One of amounts $\mathbf{x_1}$ and $\mathbf{x_8}$ must be nonzero

$$\begin{cases} x_1^c + x_5^c + x_8^c \geq (n+1)bb_i \\ \\ bb_i \leq x_1^c + x_8^c \leq 2nbb_i \end{cases}$$

Counting the Linearly Active S-boxes

- **Table 7.** Minimum number of linearly active S-boxes of standard and improved generalized Feistel structures imposed by switching properties with $n = 4$

Counting the Linearly Active S-boxes

- **Table 7.** Minimum number of linearly active S-boxes of standard and improved generalized Feistel structures imposed by switching properties with $n = 4$

round	Feistel	CLEFIA	GFS_6^{std}	GFS_6^{imp}	GFS_8^{std}	GFS_8^{imp}	GFS_{10}^{std}	GFS_{10}^{imp}	GFS_{12}^{std}	GFS_{12}^{imp}
1	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1
3	5	5	5	5	5	5	5	5	5	5
4	5	8	8	8	8	8	8	8	8	8
5	7	10	10	10	10	10	10	11	10	11
6	10	15	16	16	16	16	16	16	16	16
7	11	16	18	22	18	22	18	22	18	22
8	12	19	24	27	24	30	24	30	24	30
9	15	21	26	30	26	32	26	38	26	38
10	16	24	32	33	34	38	34	43	34	43
11	17	26	35	35	39	43	39	50	39	51
12	20	31	37	38	45	49	45	53	45	59
13	21	32	40	40	48	51	50	55	50	65
14	22	35	42	46	51	54	58	58	58	72
15	25	37	47	52	53	56	63	61	63	74
16	26	40	50	56	56	62	69	66	69	77
17	27	42	55	60	58	66	73	72	74	79
18	30	47	58	63	64	72	75	78	85	85
19	31	48	63	65	66	77	78	86	92	91
20	32	51	67	68	72	82	80	91	99	99
21	35	53	69	71	74	88	86	97	101	107
22	36	56	72	76	82	94	88	103	104	112
23	37	58	74	82	87	97	94	105	106	120
24	40	63	79	86	93	100	96	108	112	..

Conclusion

- Our approach decreased the number of equations and variables.

Conclusion

- Our approach decreased the number of equations and variables.
- Switching mechanism is more effective on linear cryptanalysis

Conclusion

- Our approach decreased the number of equations and variables.
- Switching mechanism is more effective on linear cryptanalysis
- Employing Switching mechanism in GFS_8 enhance the number of active S-boxes almost $\%20$ for 18 rounds.

Conclusion

- Our approach decreased the number of equations and variables.
- Switching mechanism is more effective on linear cryptanalysis
- Employing Switching mechanism in GFS_8 enhance the number of active S-boxes almost $\%20$ for 18 rounds.
- Two different MDS matrices in GFS_8^{imp} leads to 3 lower differentially active S-boxes rather than 4 matrices after 24 rounds.

References I

K. Shibutani.
On the diffusion of generalized Feistel structures regarding differential and linear cryptanalysis.
In SAC 2010, volume 6544, pages 211-228. Springer-Verlag, 2011.

T. Shirai and K. Shibutani.
On feistel structures using a diffusion switching mechanism.
In *FSE 2006*, volume 4046, pages 41–56. Springer-Verlag, 2006.

M. Sajadieh, A. Mirzaei, H. Mala, and V. Rijmen.
A new counting method to bound the number of active s-boxes in Rijndael and 3d.
Designs, Codes and Cryptography, 83(2):327–343, 2017.

Thank for your attention

Future Work

It is worth mentioning that, our approach can be generalized for other Feistel structures, and is usable in designing future block ciphers.