On Feistel Ciphers using Optimal Diffusion Mappings across Multiple Rounds

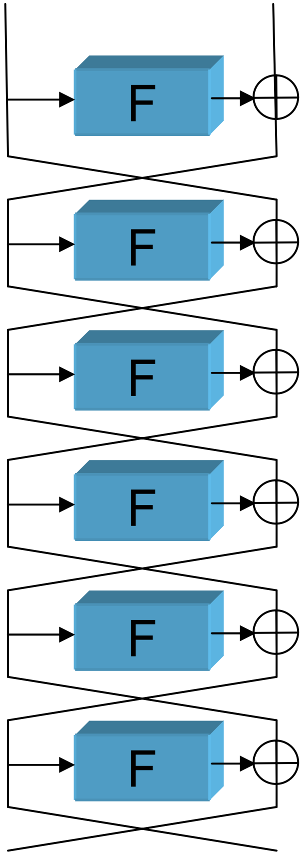
Taizo Shirai
Sony Corporation
Japan

Bart Preneel
COSIC, K.U.Leuven
Belgium

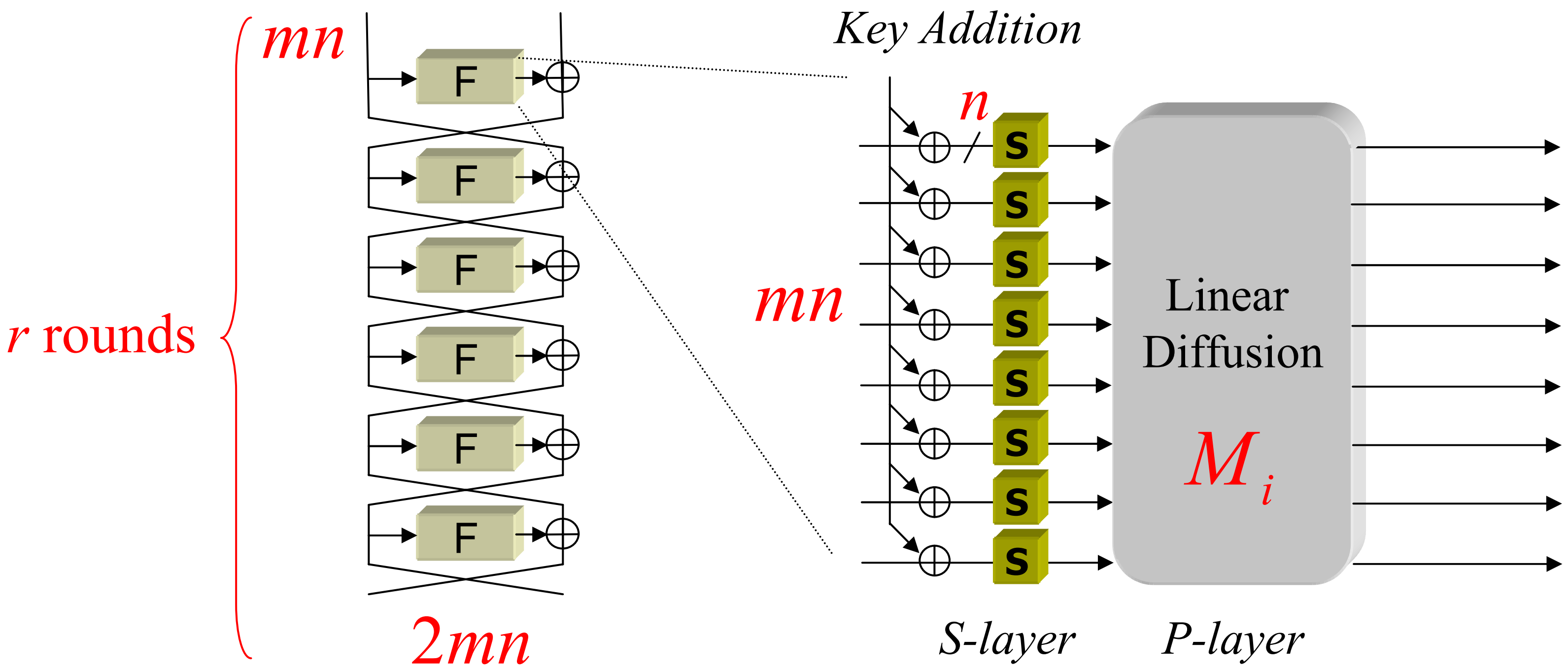
Feistel Structure

- proposed by H. Feistel (70's)
- involution property
- the F-function treats half size of block length
- tend to require more rounds than SPN structures
- used in various block ciphers

(DES, Misty, Camellia, Twofish, RC6, etc...)



Notations: $(m,n,r)-SPMFC$



m: number of S-boxes in a round

n: bit size of S-boxes

r: round number

M_i: *diffusion matrices*

Optimal Diffusion Mappings

Let $\theta:\{0,1\}^{kn}\rightarrow\{0,1\}^{ln}$ be a linear mapping,

branch number $\mathrm{B}(\theta)$ is defined as

$$\mathrm{B}(\theta)=\min_{a\neq 0}\{hw_n(a)+hw_n(\theta(a))\}$$

- If $\mathrm{B}(\theta)=l+1$, θ is called an 'optimal diffusion mapping'
  e.g. $\theta:\{0,1\}^{40}\rightarrow\{0,1\}^{40}, n=8, k=5, l=5$

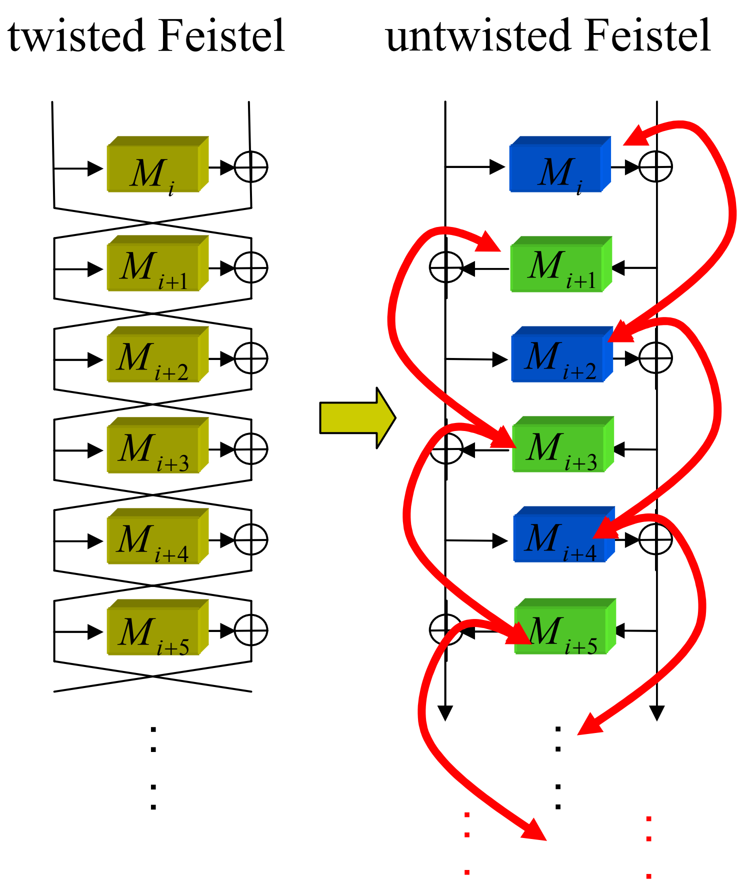
$$\begin{pmatrix} 87_x \\ 00 \\ 5f_x \\ 00 \\ b4_x \end{pmatrix} \rightarrow \boxed{\theta} \rightarrow \begin{pmatrix} 00 \\ 64_x \\ 91_x \\ 3a_x \\ 00 \end{pmatrix}$$

- Optimal diffusion mappings can be found in the generation matrices of MDS codes (Coding theory)

Block Cipher Design Approach

- How to make a strong cipher against differential attack and linear attack?
  - (Ideal) Rule out differentials and linear hulls with high probability
    - but, not easy to prove
  - (Practical) Rule out differential characteristic and linear characteristic with high probability
    - Guarantee many number of active S-boxes
      - Rijndael/AES (Wide Trail Strategy)
      - Feistel ciphers [Kanda'01, Shimizu'01]

Optimal Diffusion Mappings across Multiple Rounds : ODM-MR design



MDS-Feistel designs

- every M_k is an optimal diffusion

ODM-MR designs

- 2-round ODM-MR
  every $[M_k \mid M_{k+2}]$ is an optimal diffusion
- 3-round ODM-MR
  every $[M_k \mid M_{k+2} \mid M_{k+4}]$ is an optimal diffusion
- p-round ODM-MR
  every $[M_k \mid M_{k+2} \mid \cdots \mid M_{k+2p-2}]$ is an optimal diffusion

Guaranteed number of Active S-boxes of MDS-Feistel and 3-round ODM-MR

	m=4		*m=5*		*m=6*		*m=7*		*m=8*	
Round	**MDS**	**ODM(3)**	**MDS**	**ODM(3)**	**MDS**	**ODM(3)**	**MDS**	**ODM(3)**	**MDS**	**ODM(3)**
1	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	1
3	2	2	2	2	2	2	2	2	2	2
4	5	5	6	6	7	7	8	8	9	9
5	6	6	7	7	8	8	9	9	10	10
6	7	10	8	12	9	14	10	16	11	18
7	8	10	9	12	10	14	11	16	12	18
8	11	12	13	14	15	16	17	18	19	20
9	12	15	14	18	16	21	18	24	20	27
10	13	16	15	18	17	22	19	24	21	28
11	14	17	16	20	18	23	20	26	22	29
12	17	20	20	24	23	28	26	32	29	36
:	:	:	:	:	:	:	:	:	:	:
15	20	25	23	30	26	35	29	40	32	45
:	:	:	:	:	:	:	:	:	:	:
18	25	30	29	36	33	42	37	48	41	54

Previous Results (FSE 2004)

- *2-round ODM-MR design*
  - is better than MDS-Feistel
- *3-round ODM-MR design*
  - is better than 2-round ODM-MR and MDS-Feistel
- *p-round ODM-MR (p > 3)*
  - is as good as 3-round ODM-MR

⇨ 3-round ODM-MR design holds attractive property!

Our Main Contribution

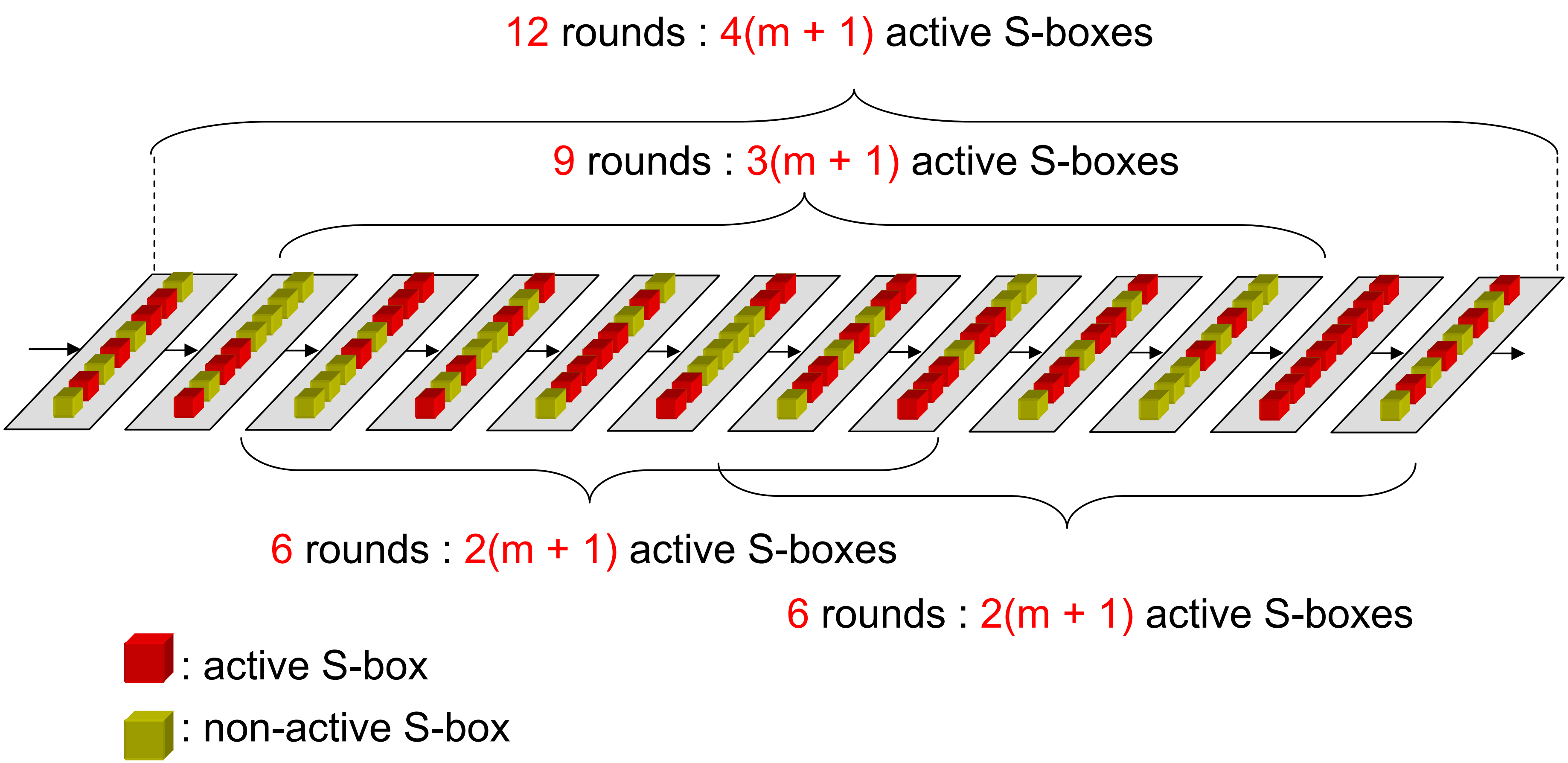
We proved the Theorem 1,2 then obtained the following corollary

Corollary

Let E be a (m,n,r)-SPMFC block cipher.

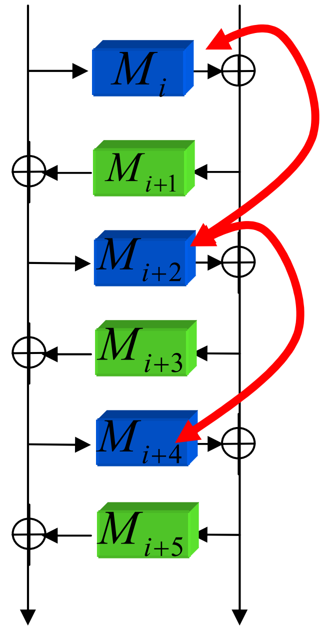
If $[M_i | M_{i+2} | M_{i+4}]$ *and* $[{}^tM_j^{-1} | {}^tM_{j+2}^{-1}]$ *are optimal diffusion mappings for any i, j, then any consecutive 3R-rounds (R ≧ 2) in E guarantee at least R(m + 1) differentially and linearly active S-boxes.*

Corollary


12 rounds : 4(m + 1) active S-boxes
9 rounds : 3(m + 1) active S-boxes
6 rounds : 2(m + 1) active S-boxes
6 rounds : 2(m + 1) active S-boxes
: active S-box
: non-active S-box

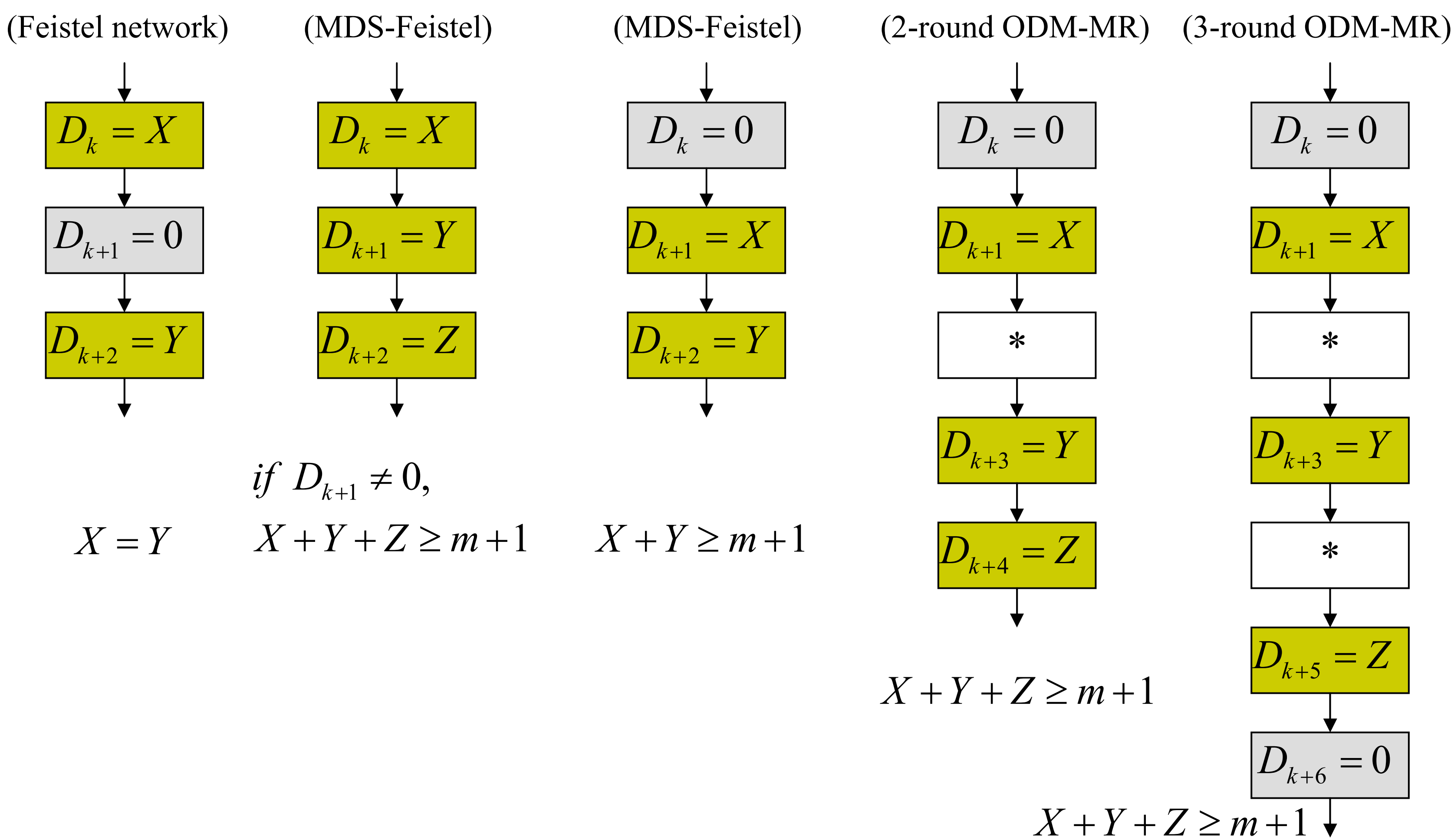
Theorem 1

If every $[M_i \,|M_{i+2}\, |M_{i+4}]$ are optimal diffusion mappings for any i, any consecutive $3R$-rounds ($R \geq 2$) in E guarantee at least $R(m + 1)$ differentially active S-boxes.

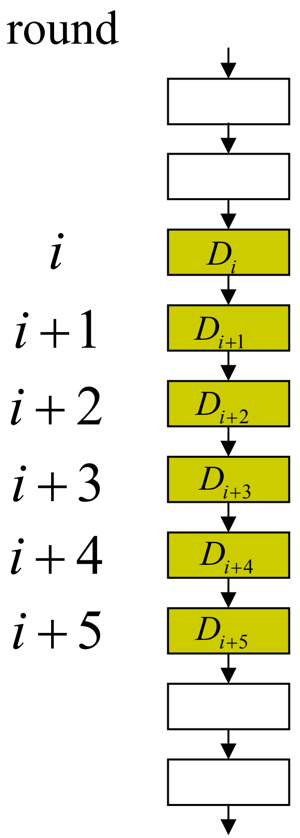


Sketch Proof of Theorem 1

- Let D_k be the number of differentially active S-boxes in the k-th round



Lemma 3 : lower bound for 6-round



2-round ODM-MR

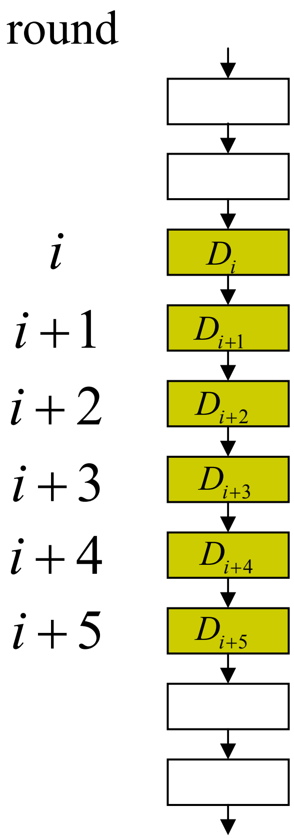
$$\underbrace{D_i + \underline{D_{i+1}} + D_{i+2}}_{\geq m+1} + \underbrace{D_{i+3} + \underline{D_{i+4}} + D_{i+5}}_{\geq m+1} \geq 2(m+1)$$

$D_{i+1} \neq 0, D_{i+4} \neq 0 \Rightarrow$

$$D_i + D_{i+1} + D_{i+2} \geq m+1,$$

$$D_{i+3} + D_{i+4} + D_{i+5} \geq m+1.$$

Lemma 3 : lower bound for 6-round



2-round ODM-MR

$$\boxed{D_i +} \; 0 \; \overbrace{+ D_{i+2} + D_{i+3}}^{\ge m+1} + D_{i+4} + D_{i+5} \ge 2(m+1)$$

$$\underbrace{+ D_{i+2} \quad + D_{i+4} + D_{i+5}}_{\ge m+1}$$

$D_{i+1} = 0 \Rightarrow$

$$D_i = D_{i+2} \,,$$

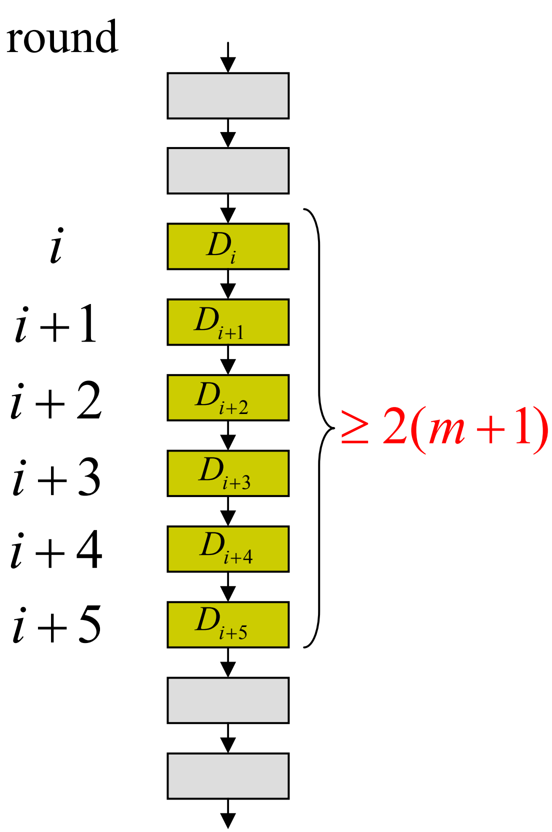
$$D_{i+2} + D_{i+3} \ge m+1 \,,$$

$$D_{i+2} + D_{i+4} + D_{i+5} \ge m+1 \,.$$

$D_{i+4} = 0 \Rightarrow$ can be proven similar manner

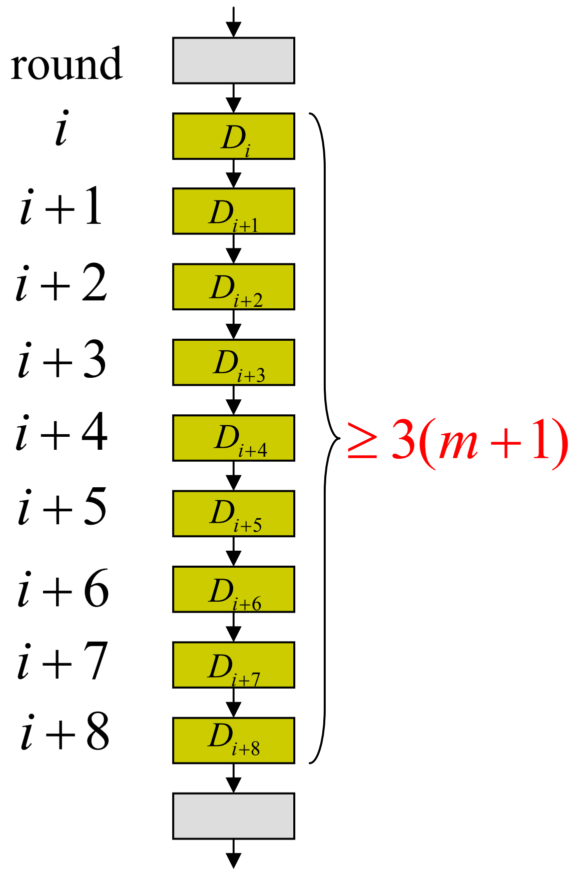
Theorem 1

Lemma 3



2-round ODM-MR

Lemma 5



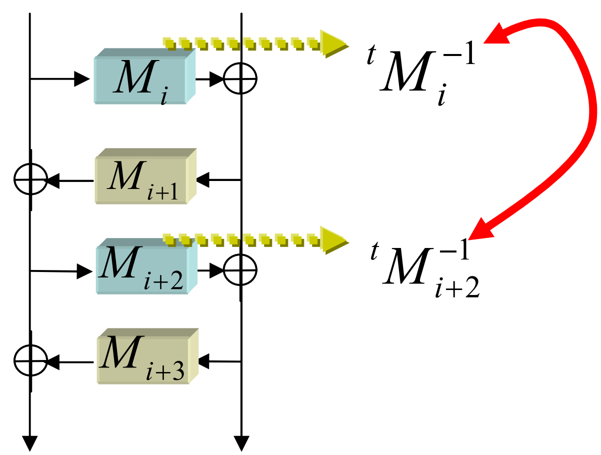
3-round ODM-MR

for 3-round ODM-MR

Any consecutive $3R$-round $(R \geq 2)$ guarantees at least $R(m+1)$ differentially active S-boxes

Theorem 2

If every $[{}^tM_j^{-1} \mid {}^tM_{j+2}^{-1}]$ are optimal diffusion mappings for any j, any consecutive $3R$-rounds in E guarantee at least $R(m + 1)$ linearly active S-boxes.



Theorem 2

- Let L_k be the number of linearly active S-boxes in the k-th round
- If every $\left[{}^{t}M_{i}^{-1} | {}^{t}M_{i+2}^{-1}\right]$ is an optimal diffusion mapping,

$L_k = X$

$L_{k+1} = Y$

$L_{k+2} = Z$

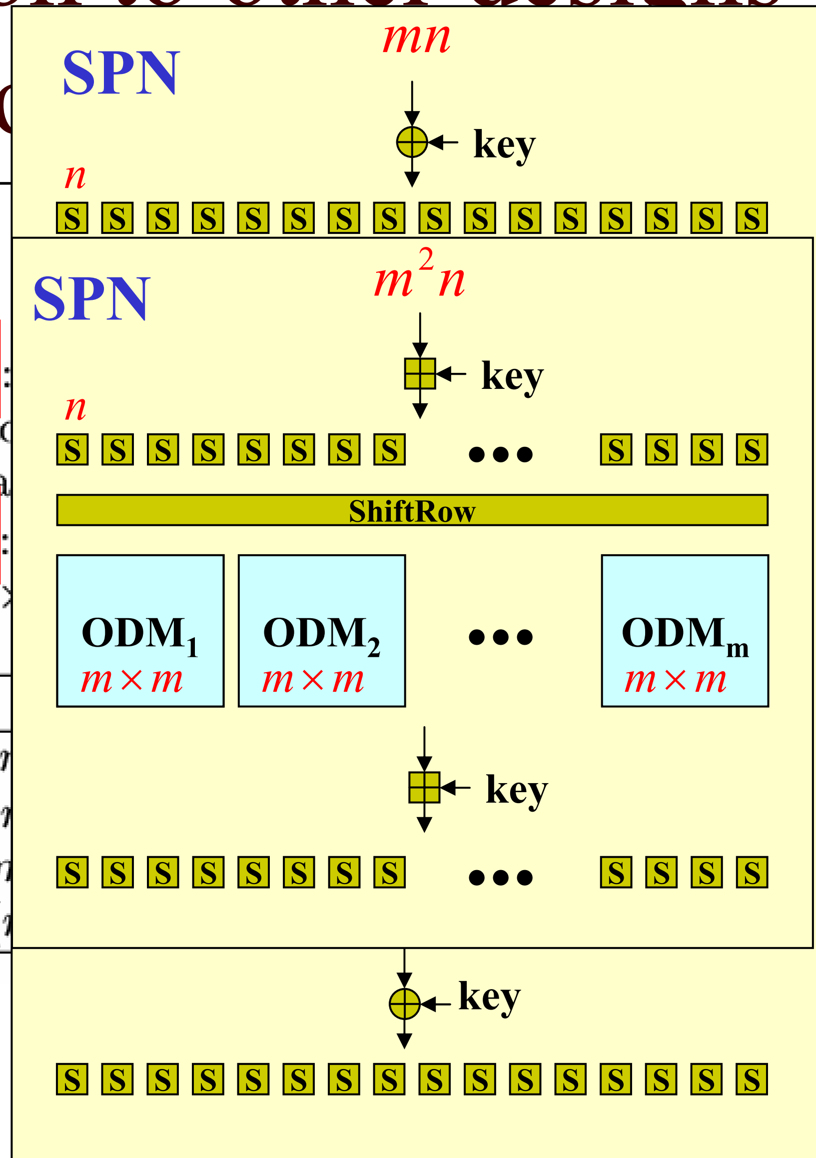
$X + Y + Z \geq m + 1$

Any consecutive $3R$-round guarantees at least $R(m+1)$ active S-boxes

Guaranteed number of Active S-boxes

	m=4			*m=5*			*m=6*			*m=7*			*m=8*		
Round	***MDS***	***D***	***L***	***MDS***	***D***	***L***	***MDS***	***D***	***L***	***MDS***	***D***	***L***	***MDS***	***D***	***L***
1	0	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	1
3	2	2	5	2	2	6	2	2	7	2	2	8	2	2	9
4	5	5	5	6	6	6	7	7	7	8	8	8	9	9	9
5	6	6	6	7	7	7	8	8	8	9	9	9	10	10	10
6	7	10	10	8	12	12	9	14	14	10	16	16	11	18	18
7	8	10	10	9	12	12	10	14	14	11	16	16	12	18	18
8	11	12	11	13	14	13	15	16	15	17	18	17	19	20	19
9	12	15	15	14	18	18	16	21	21	18	24	24	20	27	27
10	13	16	15	15	18	18	17	22	21	19	24	24	21	28	27
11	14	17	16	16	20	19	18	23	22	20	26	25	22	29	28
12	17	20	20	20	24	24	23	28	28	26	32	32	29	36	36
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
15	20	25	25	23	30	30	26	35	35	29	40	40	32	45	45
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
18	25	30	30	29	36	36	33	42	42	37	48	48	41	54	54

Comparison to other designs based on active S-bo



Rijndael type : … e round function con-
sists of key-ad … lixColumn employing
m $m \times m$ ma … tion [20].

SHARK type : … e m parallel n-bit S-
boxes, an m × … 3]

Type	…	. $\lim_{r \to \infty}$	$\lim_{m,r \to \infty}$
MDS-Feistel	(r …	0.313	0.25
ODM-MR	(r …	0.371	0.33
Rijndael type	(r …	0.391	0.25
SHARK type	(r …	0.531	0.5

Conclusion

- First showed theorems on the ODM-MR design approach
- Compared the ODM-MR design to other design approach, and confirmed an effectiveness of the ODM-MR design