The 128-bit Blockcipher CLEFIA

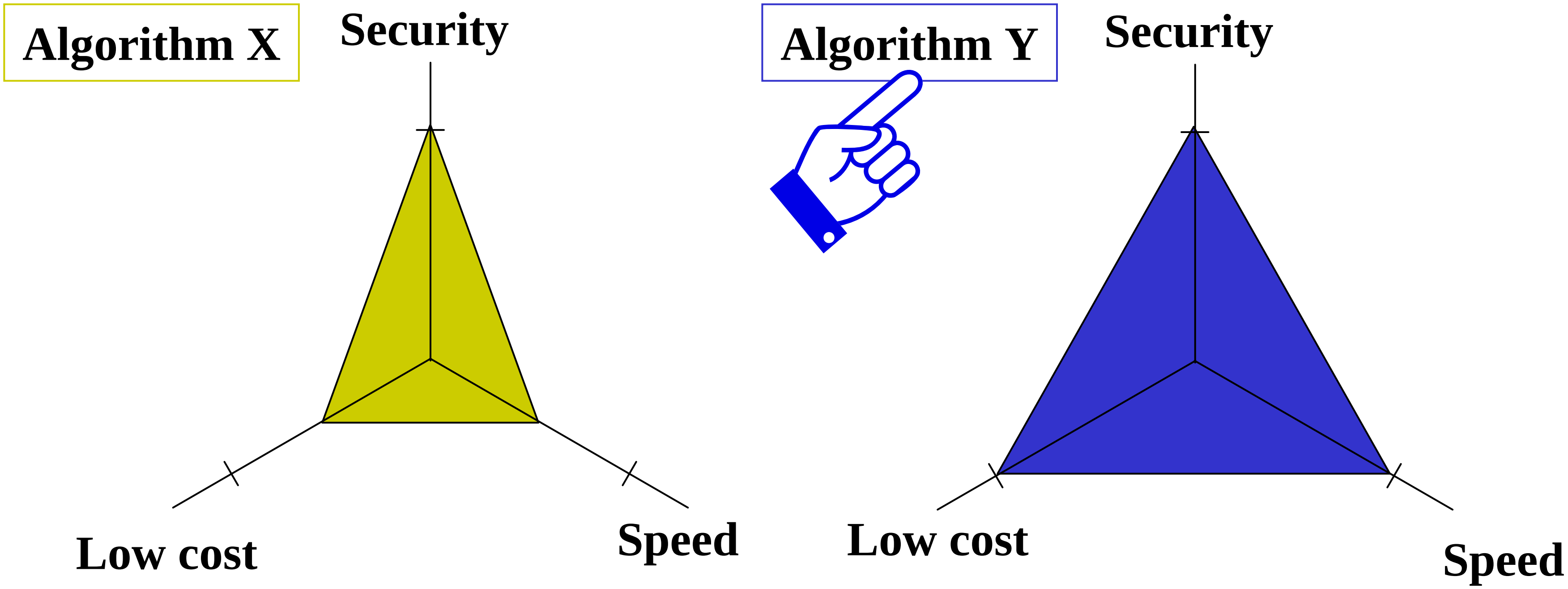
Taizo Shirai[1], Kyoji Shibutani[1], Toru Akishita[1]
Shiho Moriai[1], Tetsu Iwata[2]

[1] Sony Corporation [2] Nagoya University

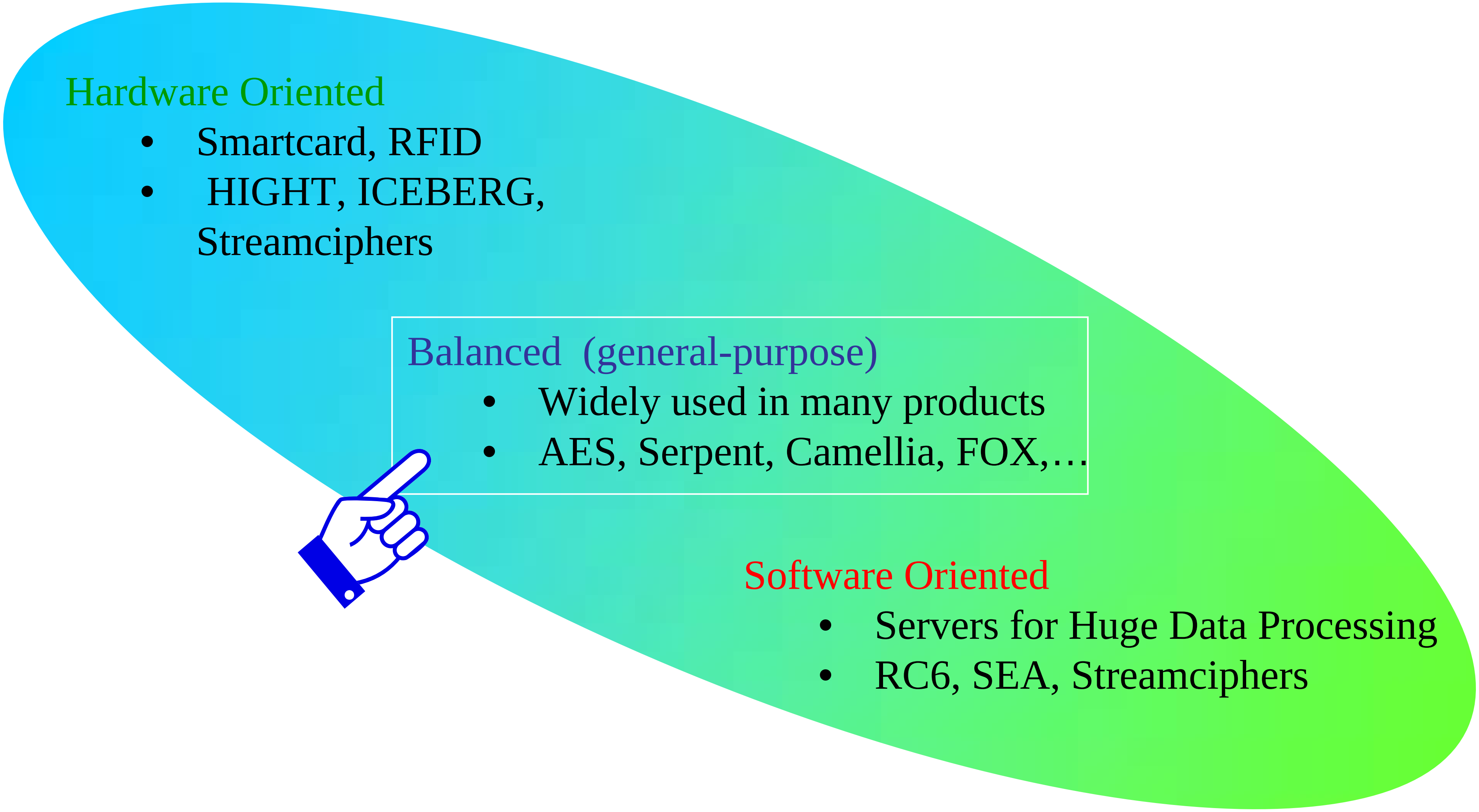
Direction for designing a new blockcipher

Priority for Choosing an algorithm

1. Security
2. Implementation cost and Encryption speed



Target Category of CLEFIA



Hardware Oriented

- Smartcard, RFID
- HIGHT, ICEBERG, Streamciphers

Balanced (general-purpose)

- Widely used in many products
- AES, Serpent, Camellia, FOX,…

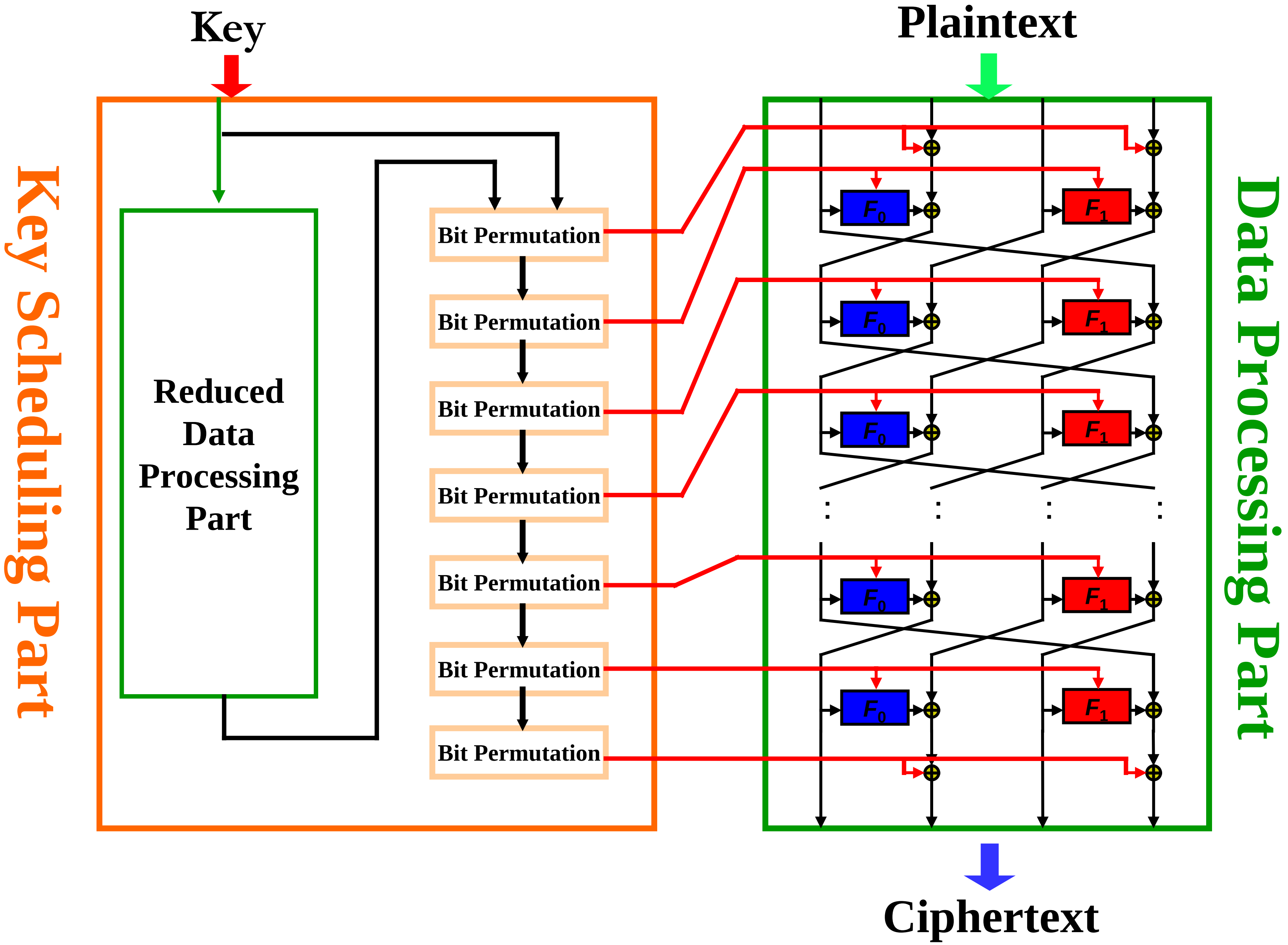
Software Oriented

- Servers for Huge Data Processing
- RC6, SEA, Streamciphers

The Blockcipher CLEFIA

Basic Information

- Block Length : 128-bit
- Key Length : 128-bit, 192-bit, 256-bit
- Structure : 4-branch generalized Feistel (Type-II)
- Number of Rounds : 18 (128-bit key),
  22 (192-bit key),
  26 (256-bit key)



Key

Plaintext

Key Scheduling Part

Reduced Data Processing Part

Bit Permutation

Bit Permutation

Bit Permutation

Bit Permutation

Bit Permutation

Bit Permutation

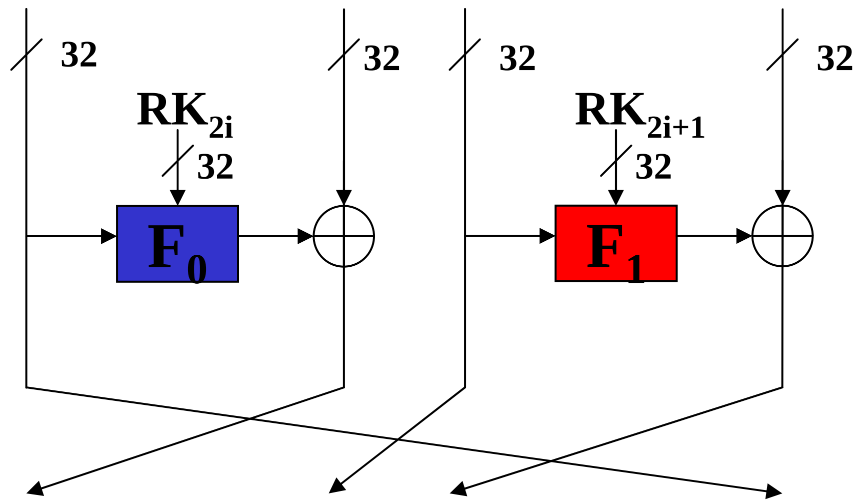
Bit Permutation

Data Processing Part

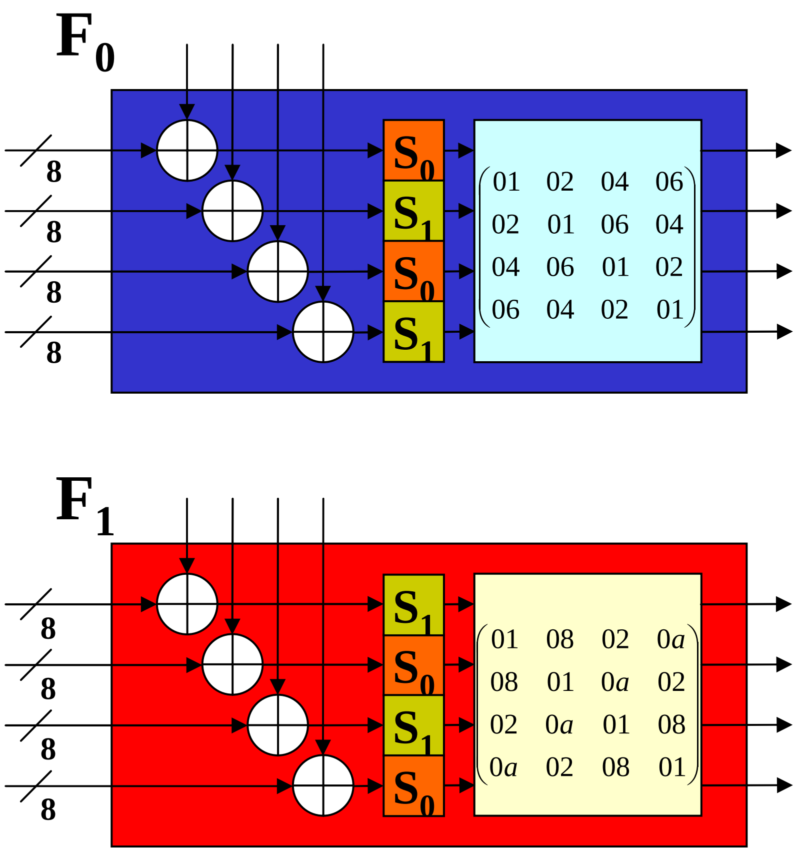
Ciphertext

SP-type F-functions

Round function



F-functions



$$\begin{pmatrix} 01 & 02 & 04 & 06 \\ 02 & 01 & 06 & 04 \\ 04 & 06 & 01 & 02 \\ 06 & 04 & 02 & 01 \end{pmatrix}$$

$$\begin{pmatrix} 01 & 08 & 02 & 0a \\ 08 & 01 & 0a & 02 \\ 02 & 0a & 01 & 08 \\ 0a & 02 & 08 & 01 \end{pmatrix}$$

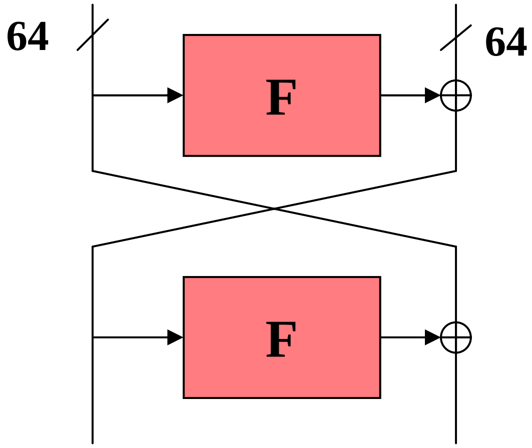
What's New in CLEFIA

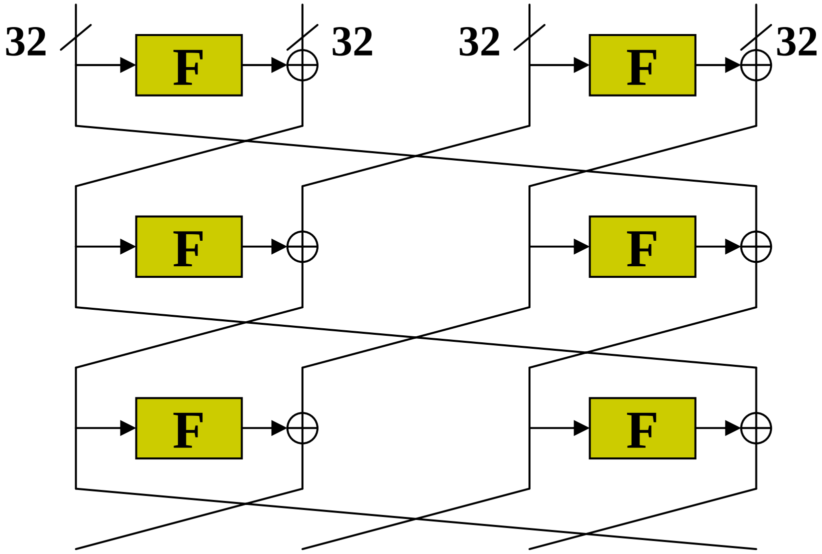
1. Combination of
   - Diffusion Switching Mechanism (DSM) , and
   - Type-II generalized Feistel structure (GFN)
2. Two S-boxes System
3. Enhanced Key Scheduling Part

2-branch Feistel VS. 4-branch Feistel

Feistel Structure

4-branch type-II generalized Feistel Structure (GFN)





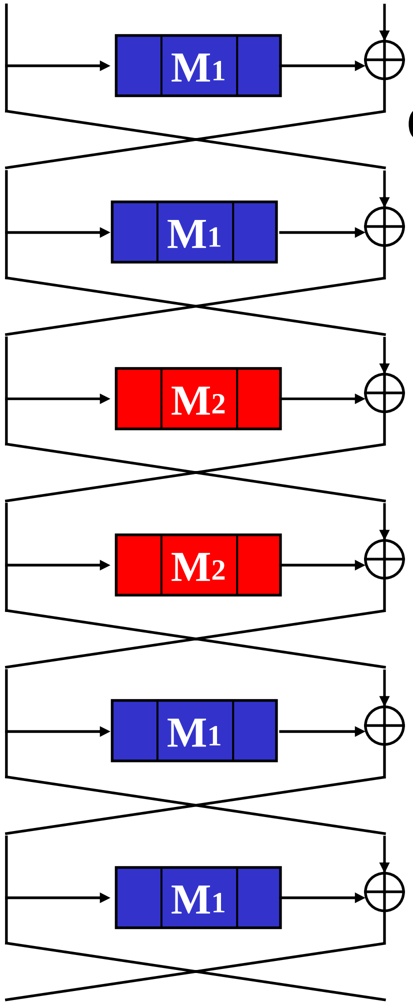
+ Better Diffusion
- Large F-function

- Slow diffusion requires more rounds
+Compact F-function

What is Diffusion Switching Mechanism (DSM)?

- DSM enhance the diffusion efficiency of Feistel structure
- To strengthen against
  - differential attack, and
  - linear attack

  by switching plural diffusion matrices in F-functions
- References
  - Shirai, Shibutani@FSE04
  - Shirai, Preneel@Asiacrypt04
  - Shirai, Shibutani@FSE06



Optimal Diffusion Mappings (MDS matrices)

M_1, M_2

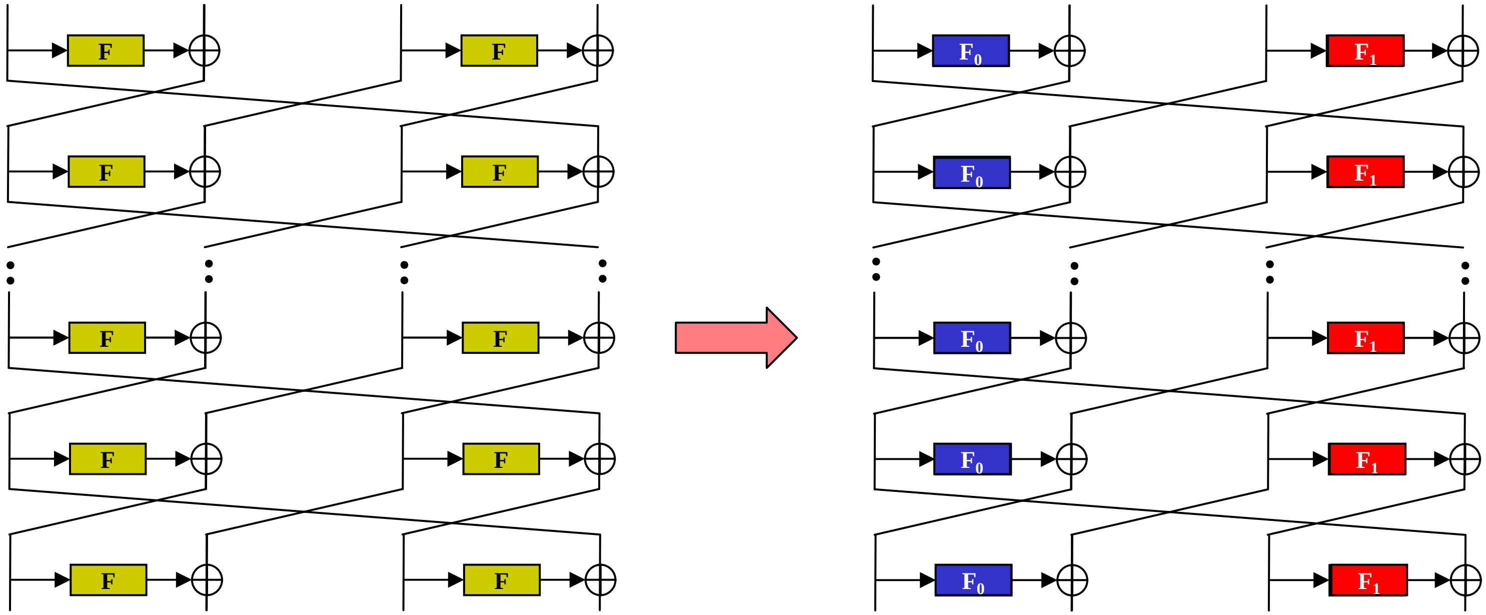
concatenation

$M_1 \| M_2$

is also an optimal diffusion mapping

4-branch GFN + DSM

- DSM is suitable to 4-branch GFN
  - No need for round depending Switching
- Effect of reducing the number of rounds
  - Reducing about 30% of number of rounds in CLEFIA’s case



Without DSM **With DSM**

Estimation of active S-boxes

S-box : S_0

$DP_{\max} = 2^{-4.67}$

$4.67 \times 28 = 130.76 > 128$

$LP_{\max} = 2^{-4.38}$

$4.38 \times 30 = 131.4 > 128$

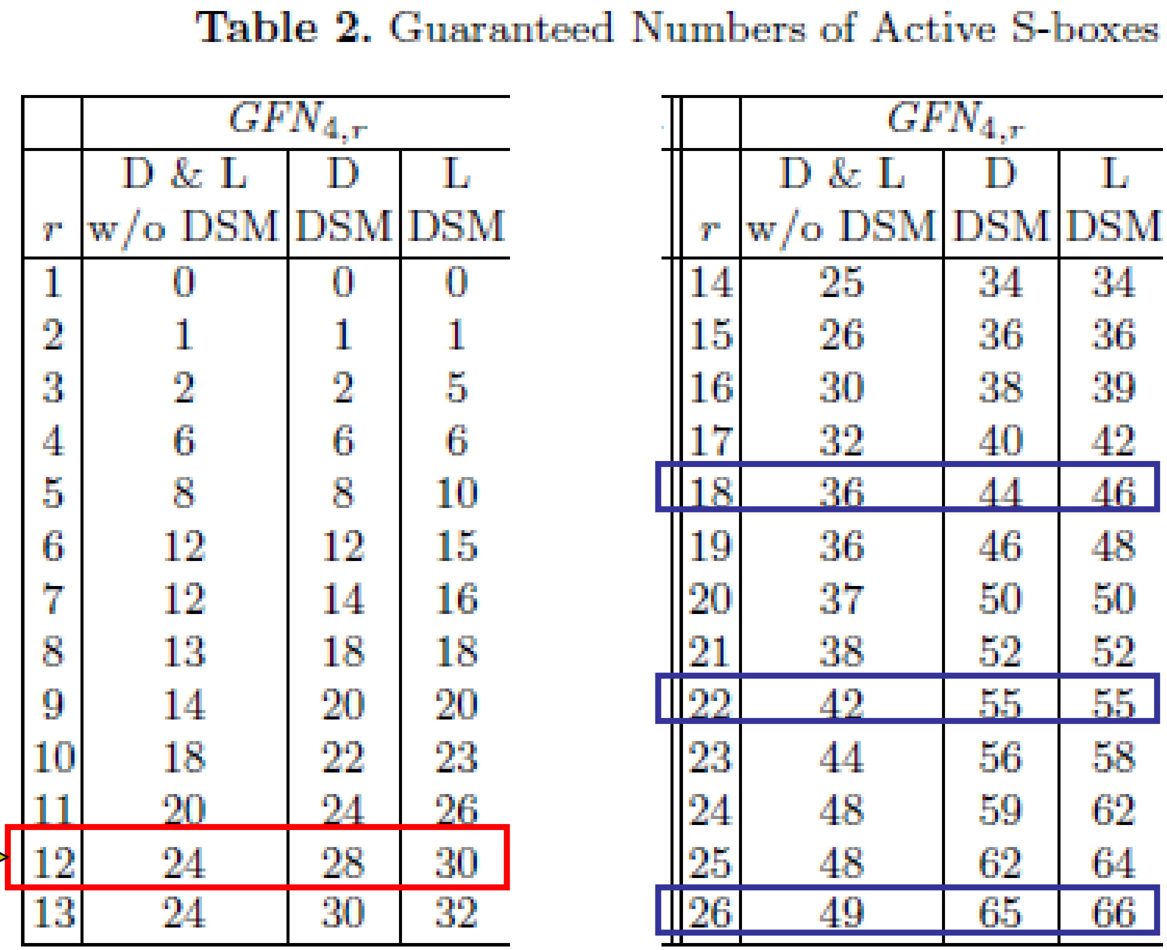


Table 2. Guaranteed Numbers of Active S-boxes

	$GFN_{4,r}$		
r	D & L w/o DSM	D DSM	L DSM
1	0	0	0
2	1	1	1
3	2	2	5
4	6	6	6
5	8	8	10
6	12	12	15
7	12	14	16
8	13	18	18
9	14	20	20
10	18	22	23
11	20	24	26
12	24	28	30
13	24	30	32
14	25	34	34
15	26	36	36
16	30	38	39
17	32	40	42
18	36	44	46
19	36	46	48
20	37	50	50
21	38	52	52
22	42	55	55
23	44	56	58
24	48	59	62
25	48	62	64
26	49	65	66

Minimum Requirement

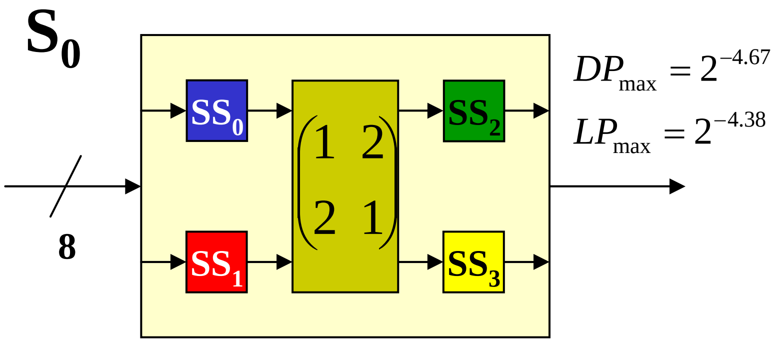
128-bit key

192-bit key

256-bit key

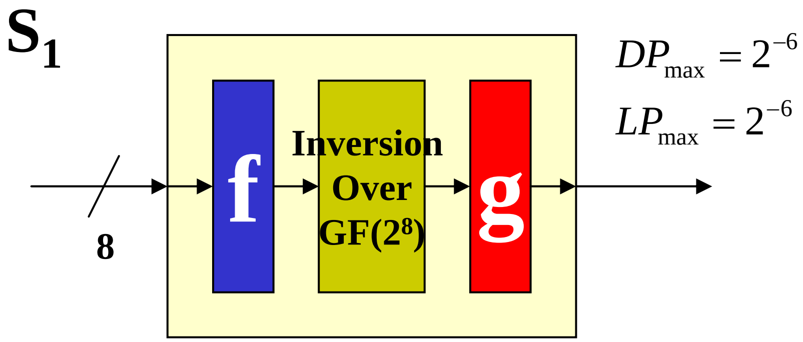
2 S-box system

- CLEFIA employs 2 different 8-bit S-boxes



$DP_{\max} = 2^{-4.67}$

$LP_{\max} = 2^{-4.38}$

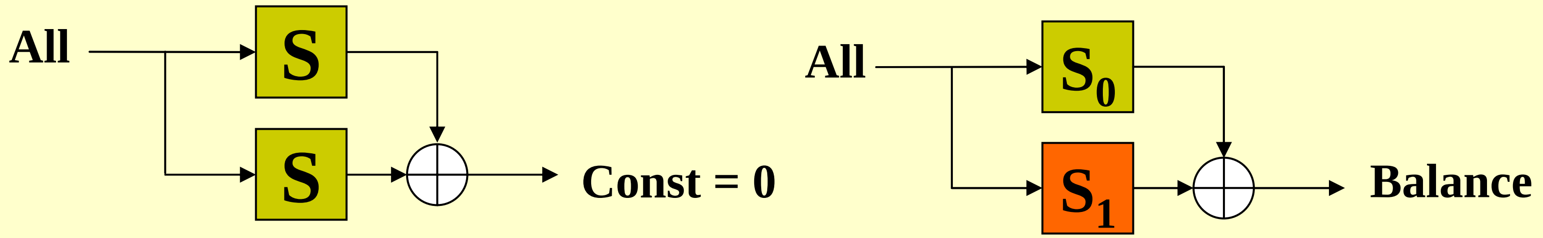


$DP_{\max} = 2^{-6}$

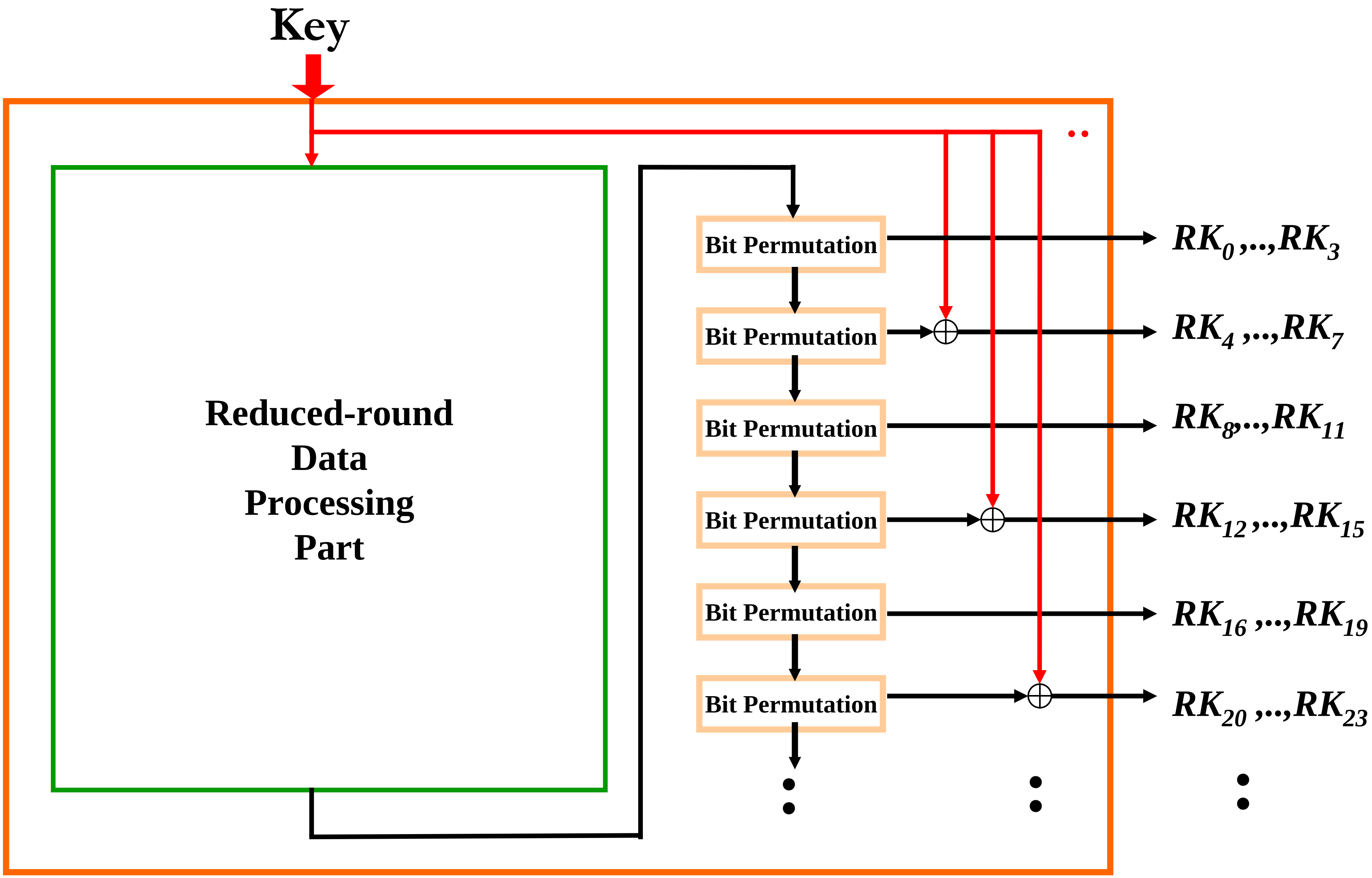
$LP_{\max} = 2^{-6}$

- **Based on 4-bit S-boxes (Whirlpool, FOX)**
- **Based on Inversion over GF(2^8) (AES, Camellia)**

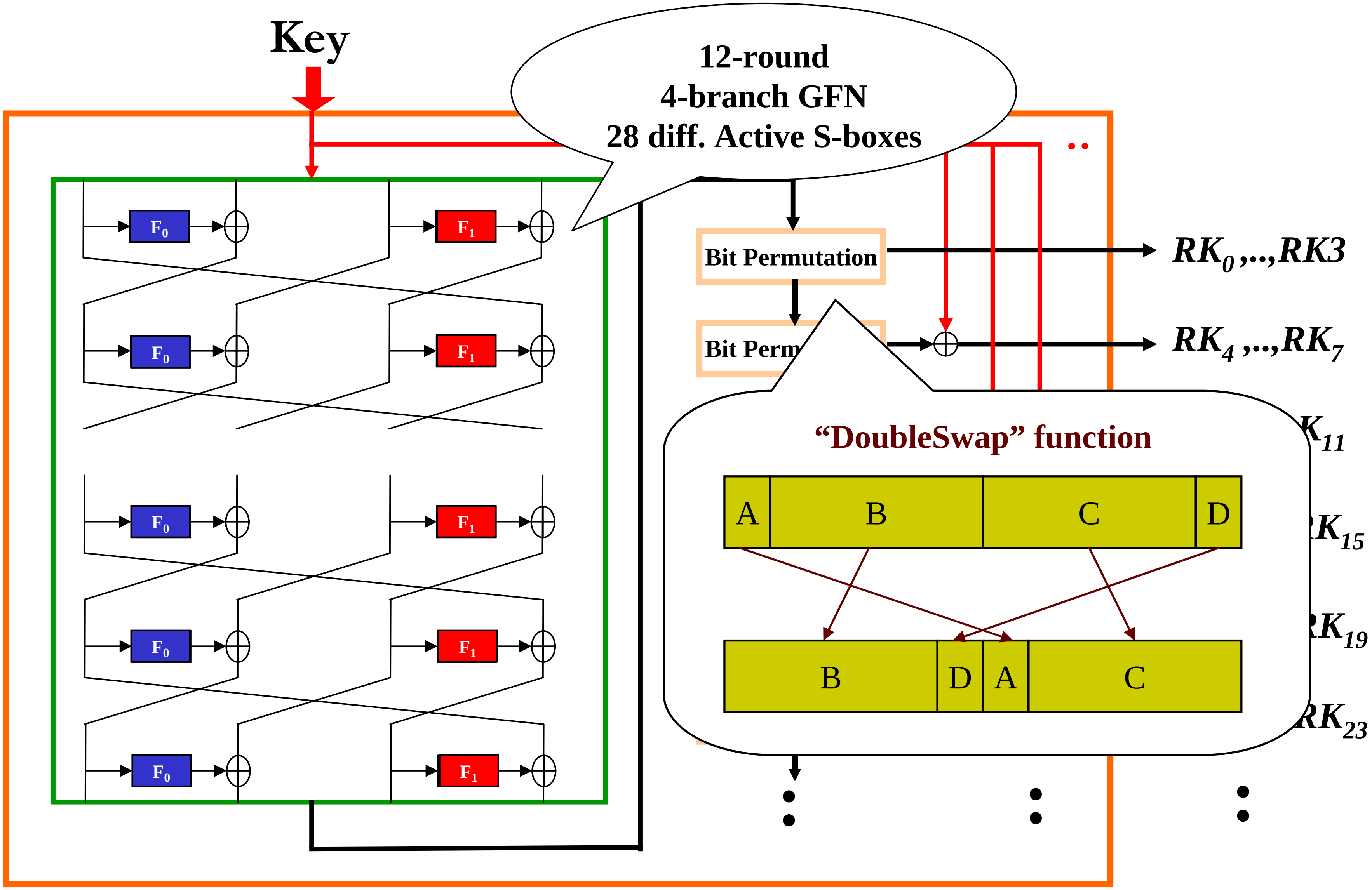
Byte oriented saturation transition



Key Scheduling Part of CLEFIA (Concept)



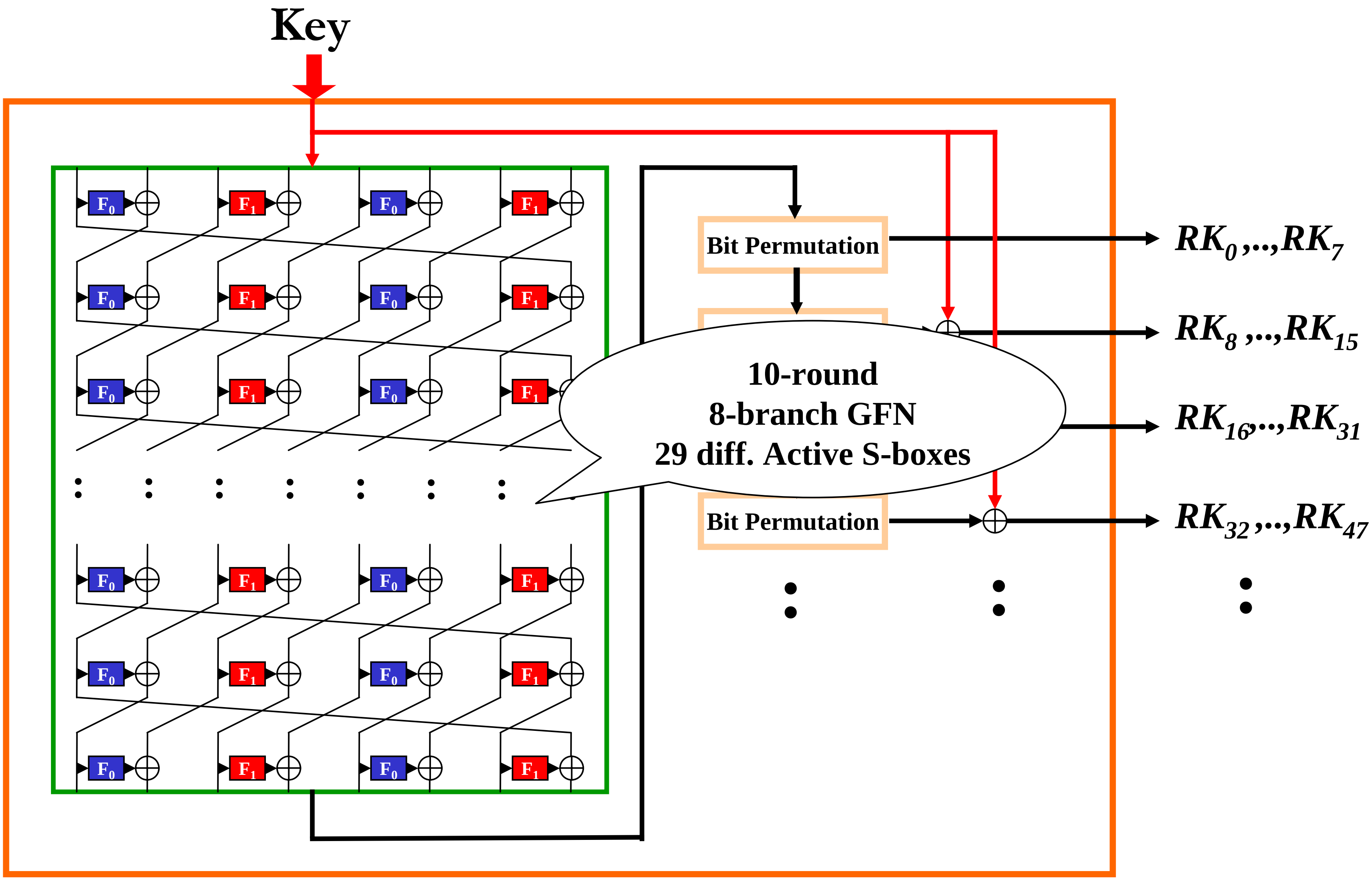
Key Scheduling Part of CLEFIA (128-bit key)



12-round
4-branch GFN
28 diff. Active S-boxes

“DoubleSwap” function

Key Scheduling Part of CLEFIA (192,256-bit key)



10-round
8-branch GFN
29 diff. Active S-boxes

Security Evaluation (excerpt)

[Data Processing Part]

- Differential Attack
  - 12-round has 28 differential active S-boxes
- Linear Attack
  - 12-round has 29 linear active S-boxes
- Impossible Differential Attack
  - Found 9-round Impossible Diff paths
- Saturation Attack
  - Found 6-round Saturation paths, 10-round attack

[Key Scheduling Part]

- Related-key type Attacks
  - Expected to be difficult due to many active S-boxes

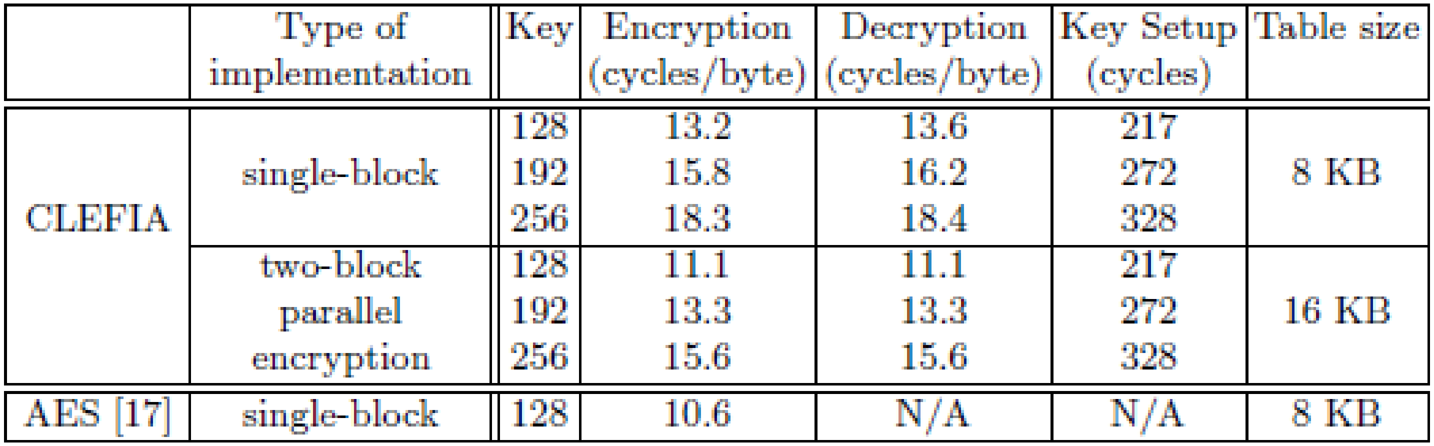
1. Differential Cryptanalysis
2. **Linear Cryptanalysis**
3. Differential-Linear Cryptanalysis
4. **Boomerang Attack**
5. Amplified Boomerang Attack
6. **Rectangle Attack**
7. Truncated Differential Cryptanalysis
8. **Truncated Linear Cryptanalysis**
9. Impossible Differential Cryptanalysis
10. **Saturation Cryptanalysis**
11. Higher Order Differential Cryptanalysis
12. **Interpolation Cryptanalysis**
13. XSL Attack
14. **Chi-Square Cryptanalysis**
15. Slide Attack
16. **Related-Cipher Cryptanalysis**
17. Related-Key Cryptanalysis
18. **Related-Key Boomerang Cryptanalysis**
19. Related-Key Rectangle Cryptanalysis
20. **Collision Attack**

Performance : Software

Estimation

- 90% of AES operations↑ + dependency↓
  - 144 S-boxes in CLEFIA vs. 160 S-boxes in AES (128-bit key)

Current Experimental Results on Athlon 64 in assembly



	Type of implementation	Key	Encryption (cycles/byte)	Decryption (cycles/byte)	Key Setup (cycles)	Table size
CLEFIA	single-block	128	13.2	13.6	217	8 KB
		192	15.8	16.2	272	
		256	18.3	18.4	328	
	two-block parallel encryption	128	11.1	11.1	217	16 KB
		192	13.3	13.3	272	
		256	15.6	15.6	328	
AES [17]	single-block	128	10.6	N/A	N/A	8 KB

Performance : Hardware

Reasons for the Compactness

- 4-branch GFN
- F-functions can be shared by Data Processing Part and Key Scheduling Part
- Small footprint S-box and Matrices

Type of Implementation	Algorithm	Cycle	Gate Size	Throughput [Mbps]	Efficiency * [Throughput / gate]	Process Rule	Ref
Compact	**CLEFIA**	**36**	**4,993**	**677**	**135**	**0.09 μm**	
	AES	**54**	**5,398**	**311**	**85.5***	**0.13 μm**	**[20]**
	Camellia	**44**	**6,511**	**325**	**75***	**0.13 μm**	**[20]**
Speed	**CLEFIA**	**18**	**6,061**	**1,424**	**235**	**0.09 μm**	
	AES	**11**	**12,454**	**1,691**	**202.5***	**0.13 μm**	**[20]**
	Camellia	**22**	**10,993**	**971**	**132***	**0.13 μm**	**[20]**

***The values of efficiency are adjusted by multiplying 1.5 by taking the difference of process into account**

Conclusion

- Proposed a new blockcipher CLEFIA
  - DSM + 4-branch Feistel, Two S-boxes, Enhanced Key Schedule, etc..
- Confirmed Potential ability for compact and fast implementations
  - Software – One of the fastest ciphers
  - Hardware – Achieved the best efficiency

  among known general-purpose blockciphers.
- Keeping enough security margin against all known attacks

Analysis of CLEFIA is very welcome!