Preimage Attacks on Reduced Tiger and SHA-2

Takanori Isobe and Kyoji Shibutani
Sony Corporation

FSE 2009, 23 February 2009

Outline

- Background
- Summary
- Preimage attack based on MITM
- Preimage attack on 16-round Tiger
- Preimage Attack on 24-step SHA-2
- Conclusion

Background

- **Preimage attacks based on the Meet-In-The-Middle approach**
  - Leurent, “MD4 is not one-way”, FSE 2008
  - Mendel, et al., “A (second) preimage attack on the GOST hash function”, FSE 2008
  - Mendel, et al., “Cryptanalysis of GOST hash function”, CRYPTO 2008
  - Aumasson, et al., “Preimage attacks on 3-pass HAVAL and step-reduced MD5”, SAC 2008
  - Aoki and Sasaki, “Preimage attack on one-block MD4, 63-step MD5 and more”, SAC 2008
  - Sasaki and Aoki, “Preimage attack on step-reduced MD5”, ACISP 2008
  - Sasaki and Aoki, “Preimage attacks on 3, 4, and 5-pass HAVAL”, ASIACRYPT 2008
  - Sasaki and Aoki, “A preimage attack for 52-step HAS-160”, ICISC 2008
- **MITM approach**
  1. Dividing round/step functions into 2 parts
  2. Finding “independent words” in the KSF (Key Scheduling Function)
- **KSF**
  - MD4 and 5: simple (word permutation)
  - Tiger and SHA-2: complicated
- **Motivation**
  - Can we find independent words in complicated KSF ?

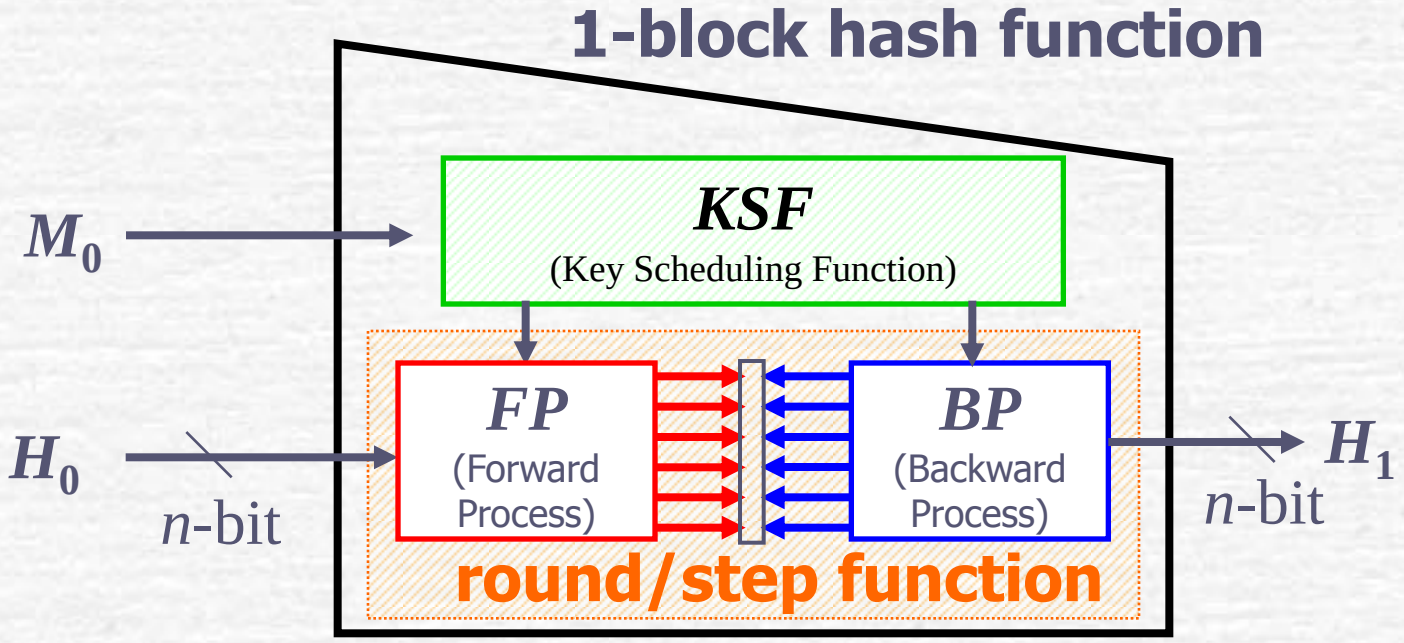
Summary

Target	Attack (1st or 2nd preimage)	Attacked steps/rounds	Complexity
Tiger (full 24 rounds)	1st Preimage [4]	13	$2^{128.5}$
	1st preimage (Ours)	16	2^{161}
	2nd preimage [4]	13	$2^{127.5}$
	2nd primage (Ours)	16	2^{161}
SHA-256 (full 64 steps)	1st preimage (Ours)	24	2^{240}
	2nd preimage (Ours)	24	2^{240}
SHA-512 (full 80 steps)	1st preiamge (Ours)	24	2^{480}
	2nd preimage (Ours)	24	2^{480}

[4] S. Indesteege and B. Preneel, "Preimagaes for reduced-round Tiger.", WEWoRC, 2007

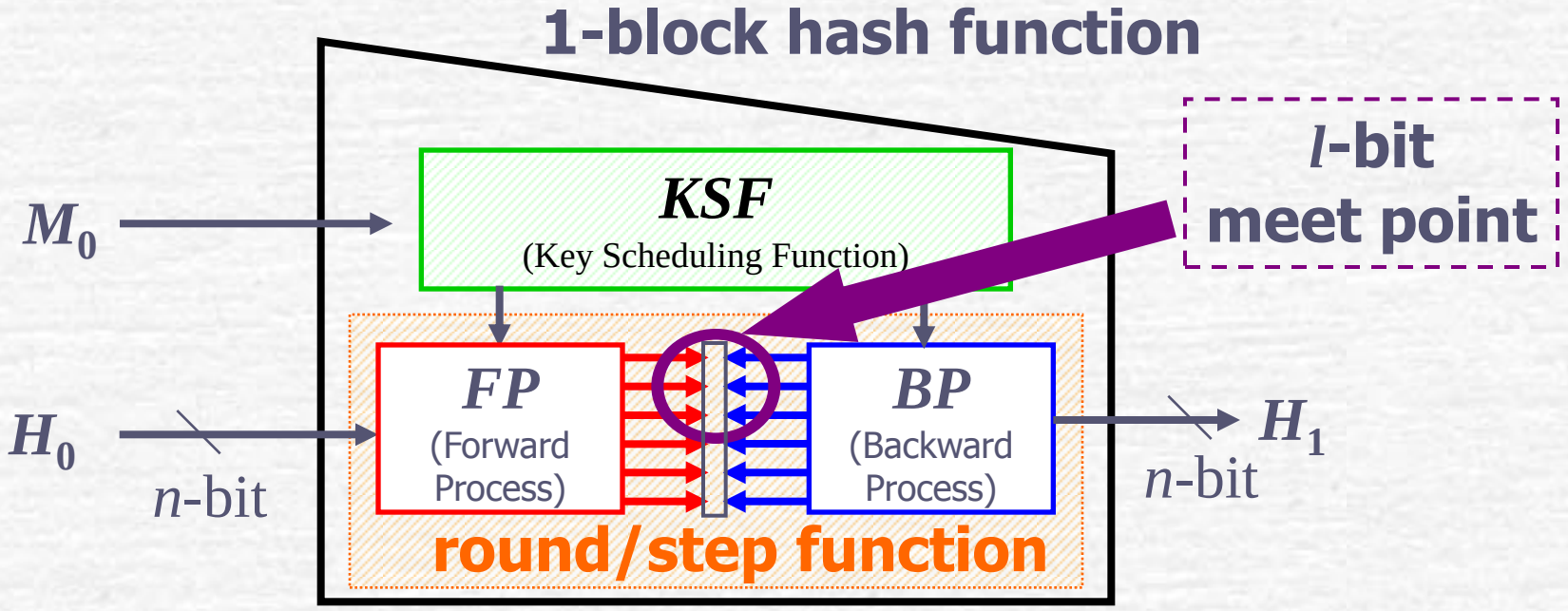
* A first preimage attack on 36-step SHA-256 was presented by Sasaki and Aoki at CRYPTO'08 rump session.

Preimage Attack based on MITM



Preimage attack: Brute force = 2^n

Preimage Attack based on MITM



Preimage attack: **Brute force** = 2^n

MITM = $2^{n - l/2}$

birthday paradox

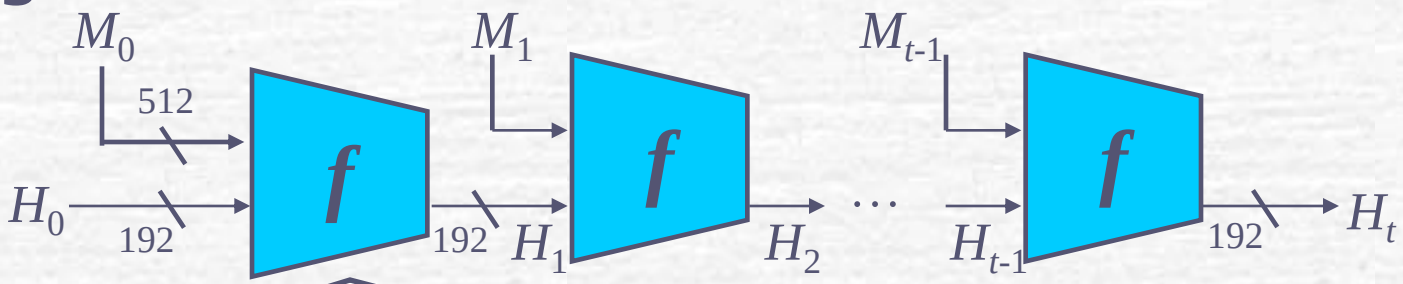
e.g.
n = 256, l = 64
Brute force = 2^{256}
MITM = 2^{224}

1. Dividing round/step function into 2 parts
2. Finding independent words in the KSF

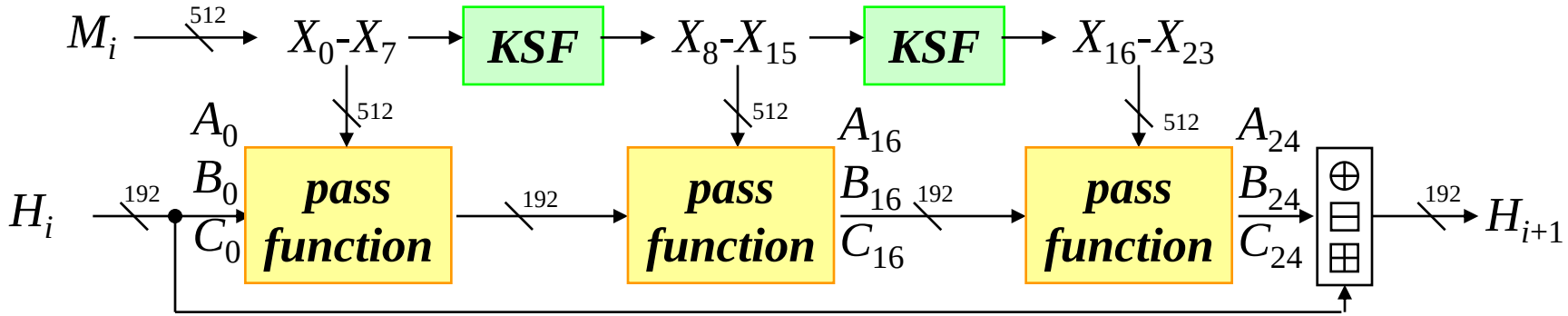
Tiger hash function

- **Tiger: 192-bit hash function designed by Anderson and Biham in 1996**

- **Tiger hash function**

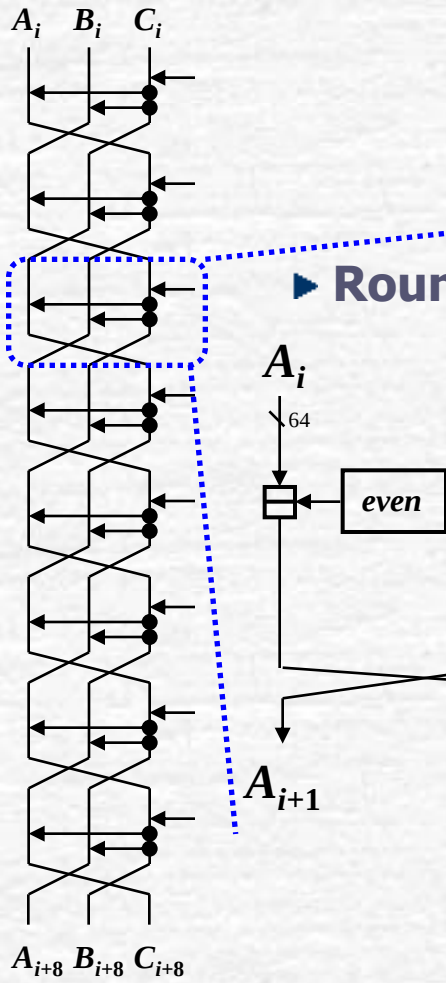


- **Compression function f (24 rounds)**

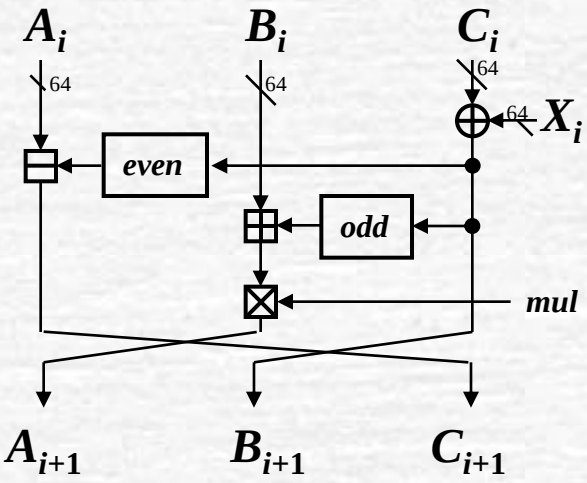


Pass function & KSF

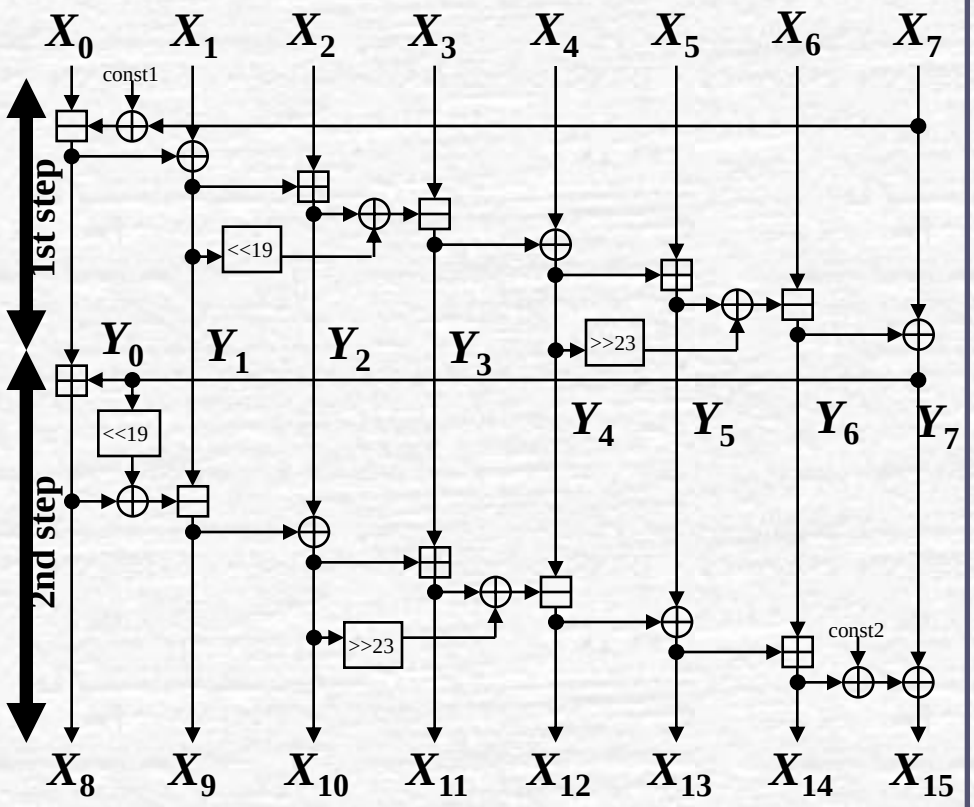
- 1 Pass function
  = 8 round functions



- Round function



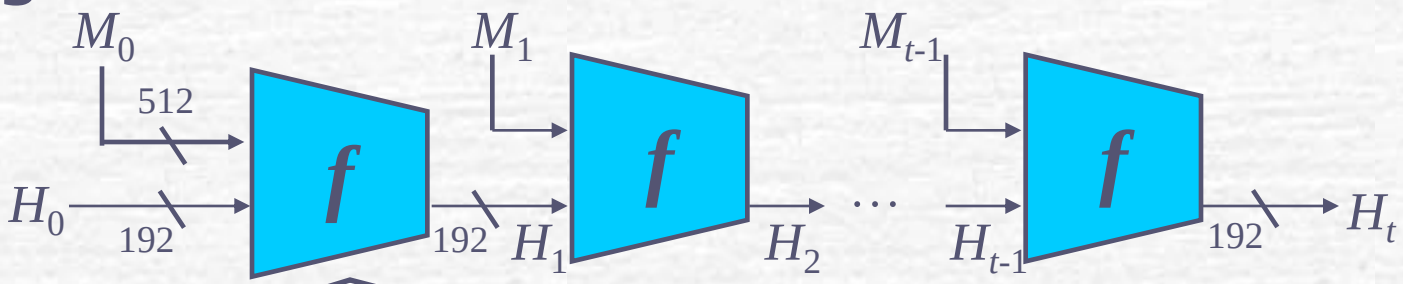
- Key scheduling function *KSF*



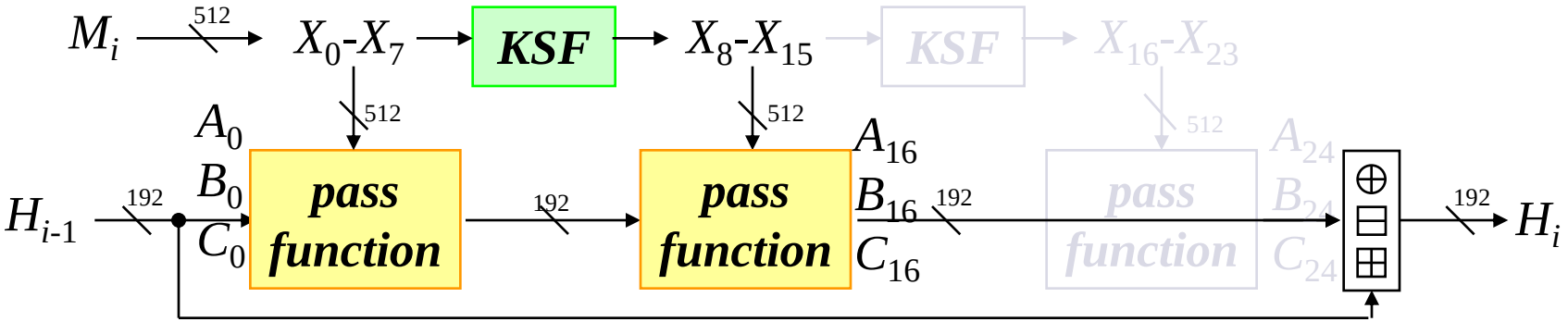
Attack Target

- **Tiger: 192-bit hash function designed by Anderson and Biham in 1996**

- **Tiger hash function**



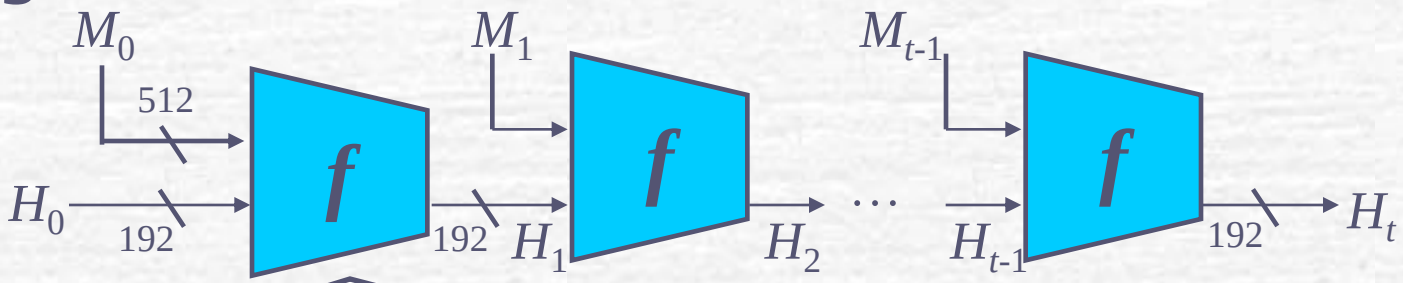
- **Compression function f (24 rounds -> 16 rounds)**



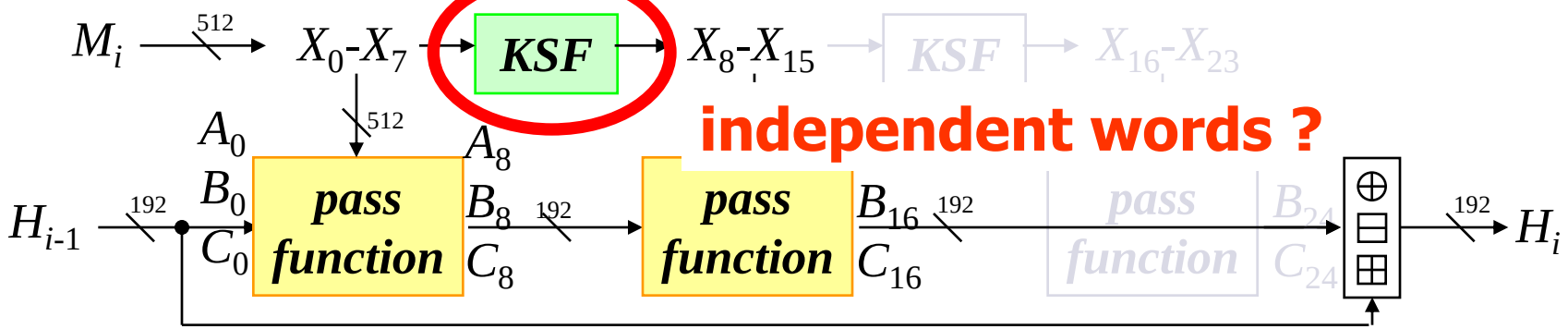
Attack Target

- **Tiger: 192-bit hash function designed by Anderson and Biham in 1996**

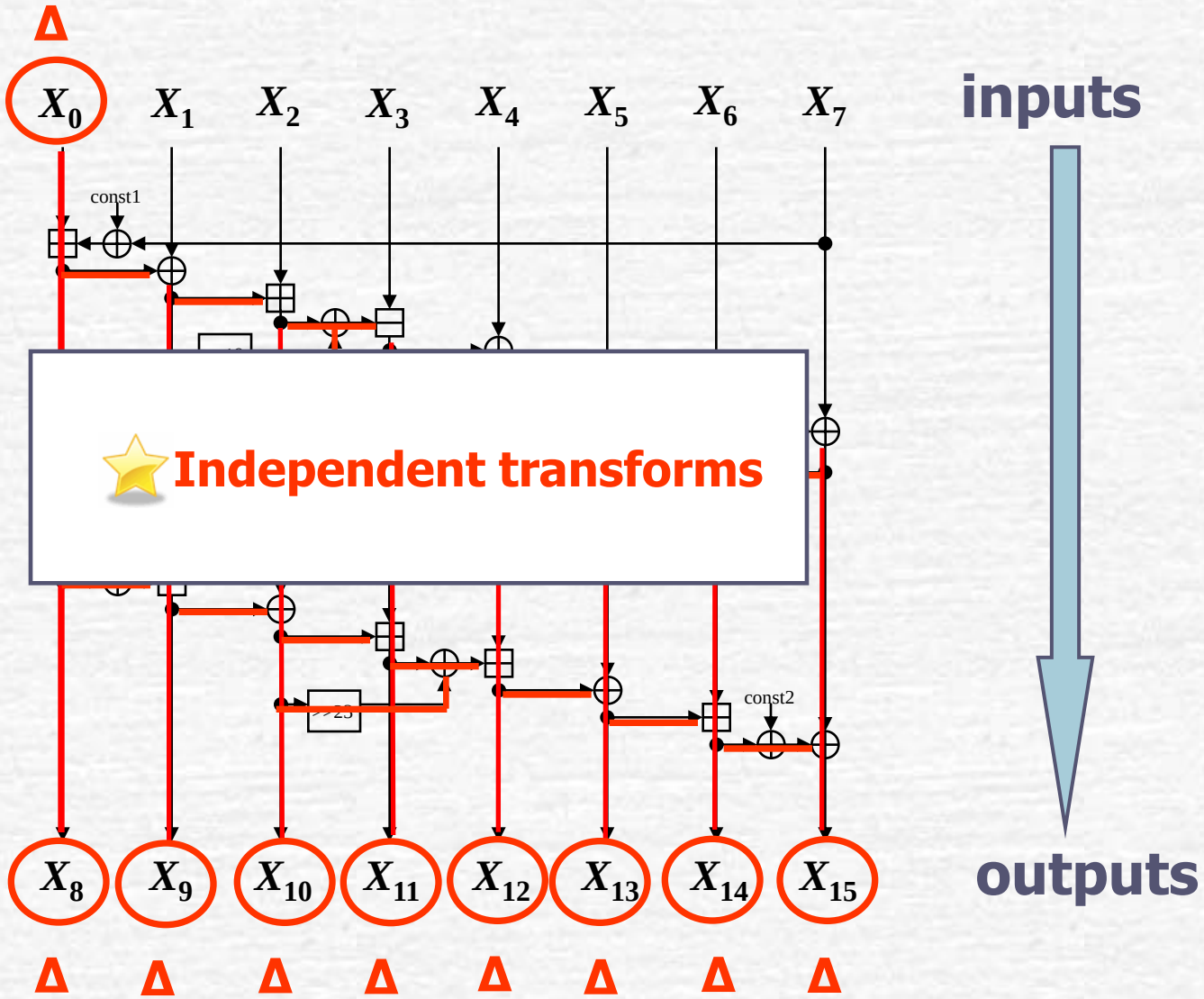
- **Tiger hash function**



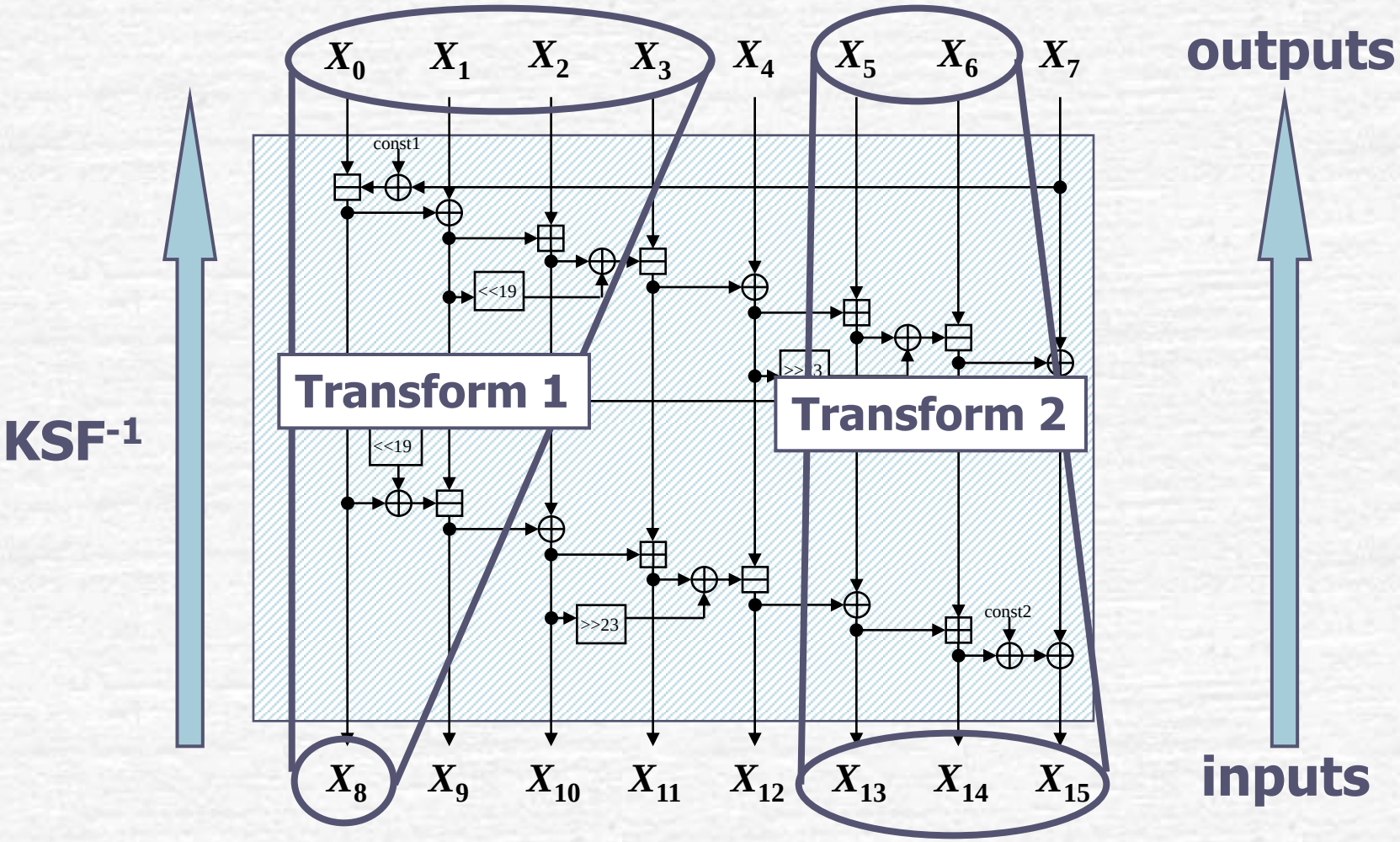
- **Compression function f (24 rounds -> 16 rounds)**



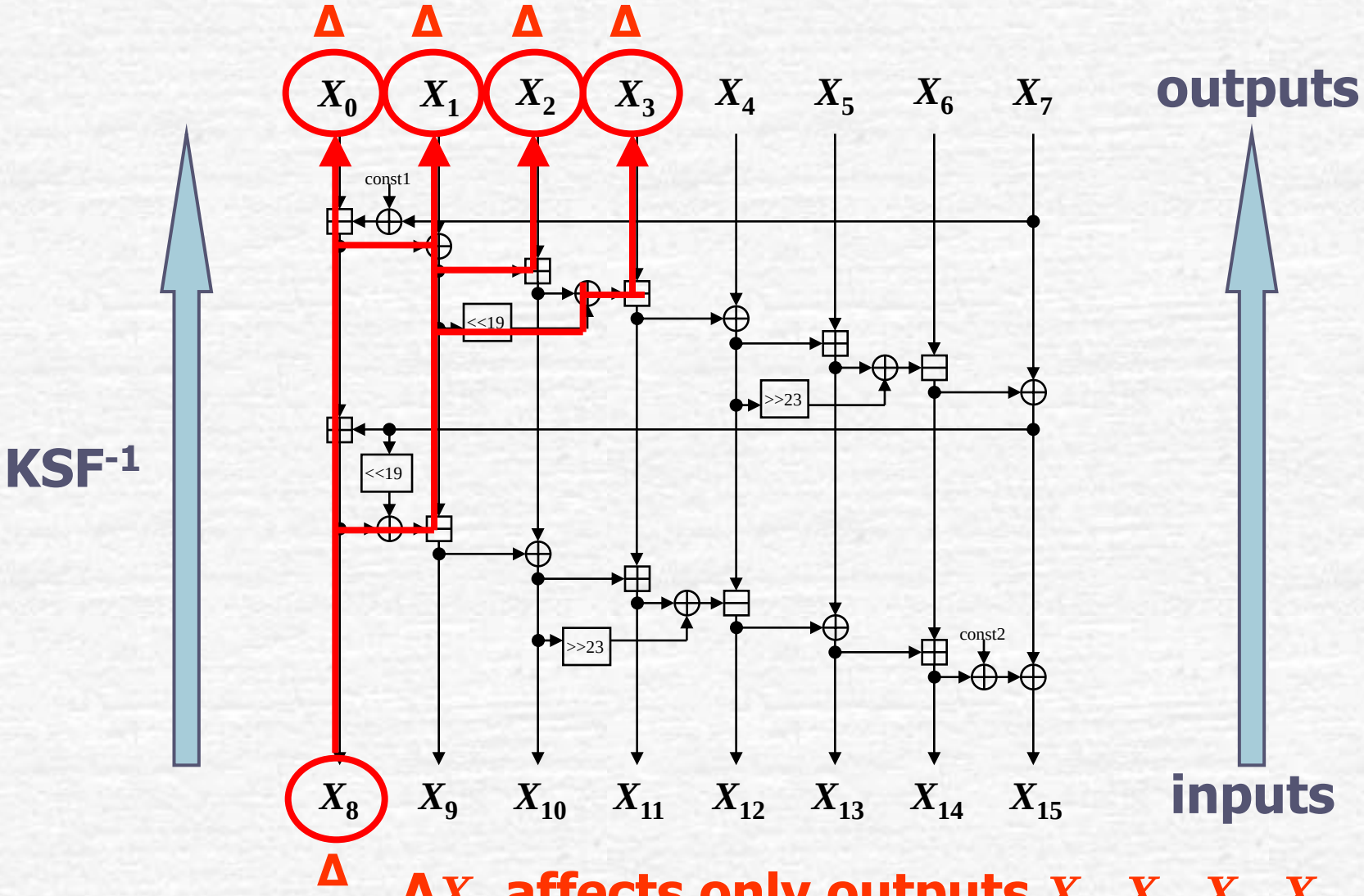
The property of KSF



Independent transforms in the KSF

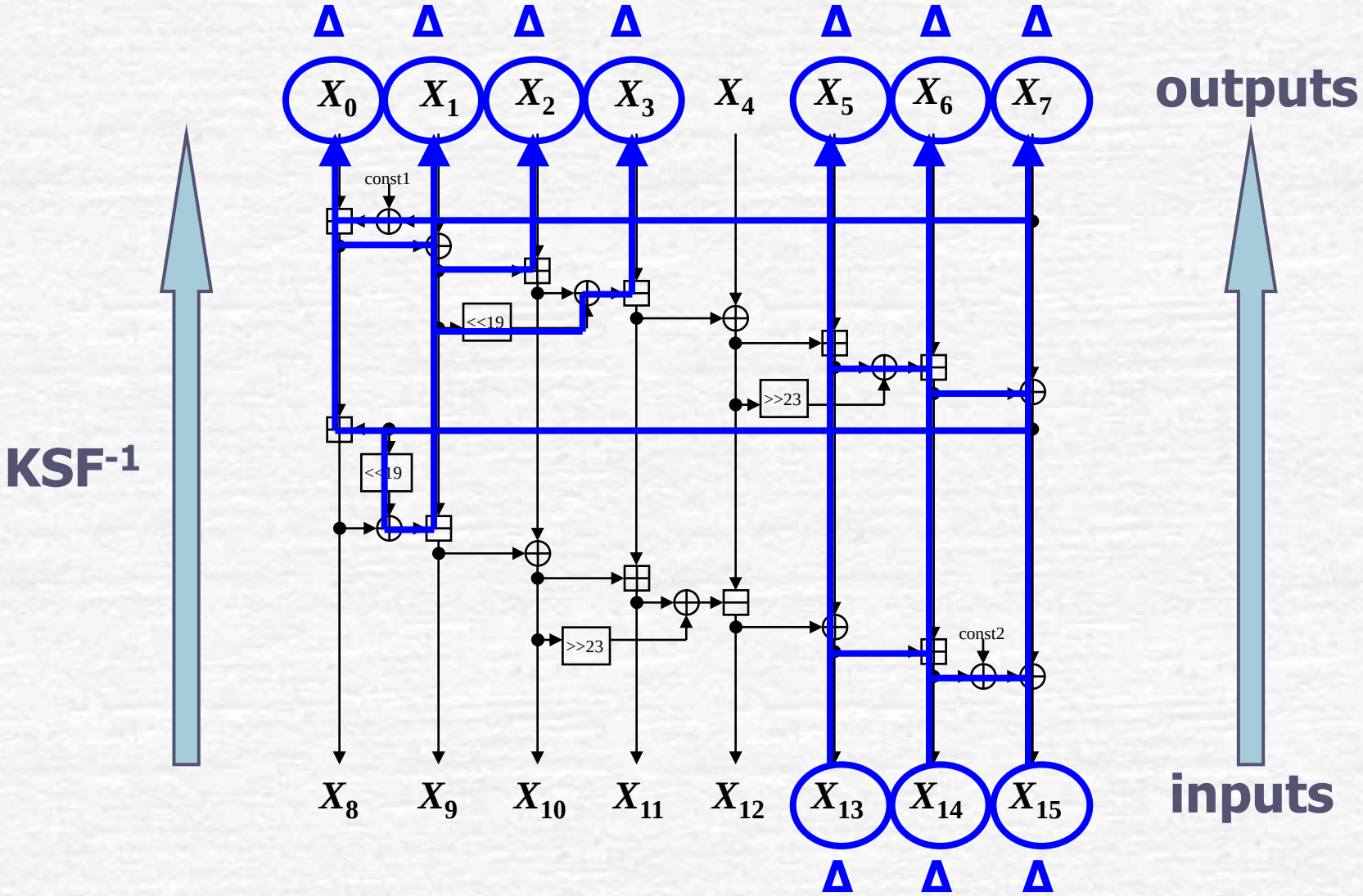


Transform 1



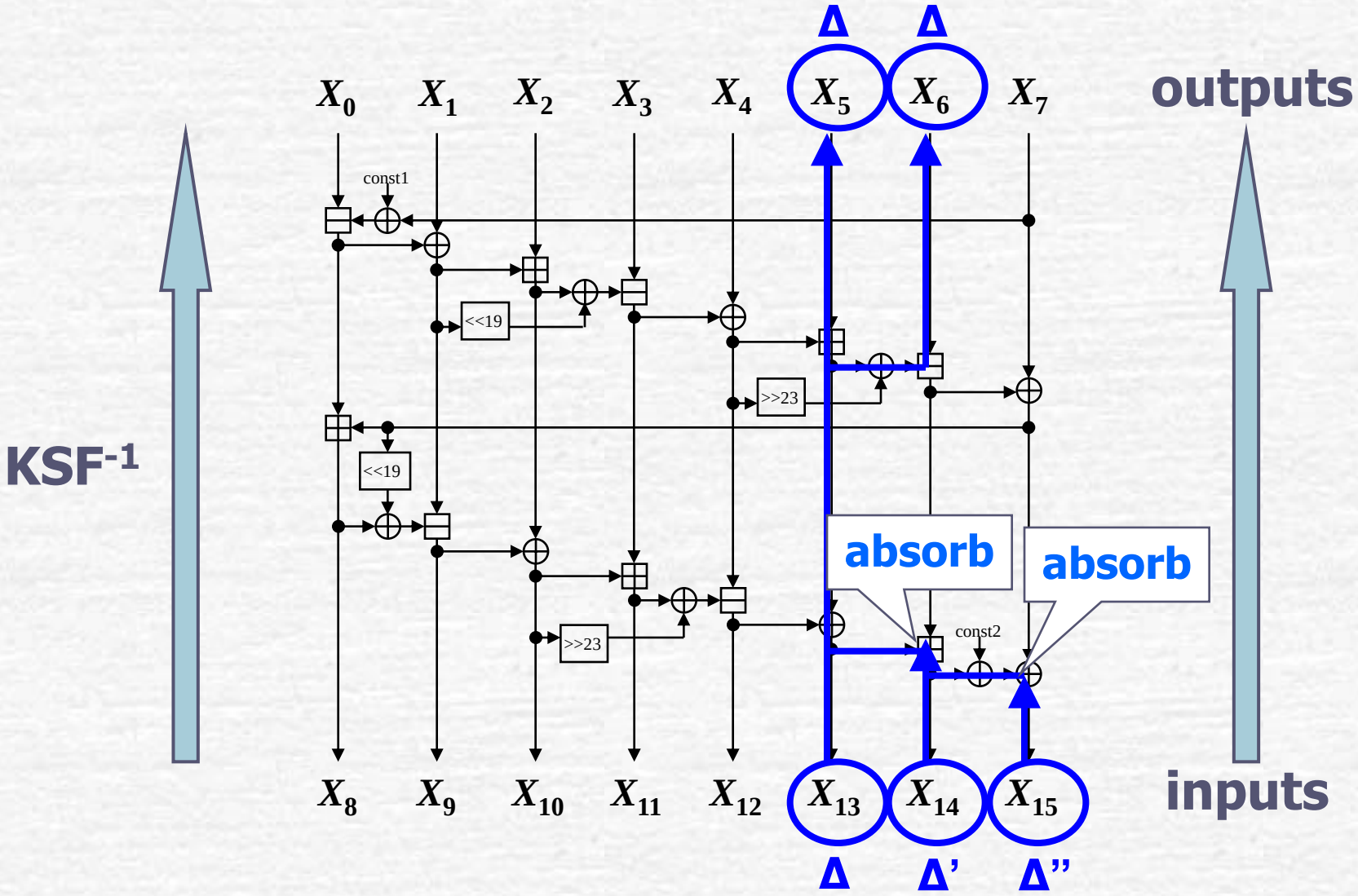
ΔX_8 affects only outputs X_0, X_1, X_2, X_3

Transform 2



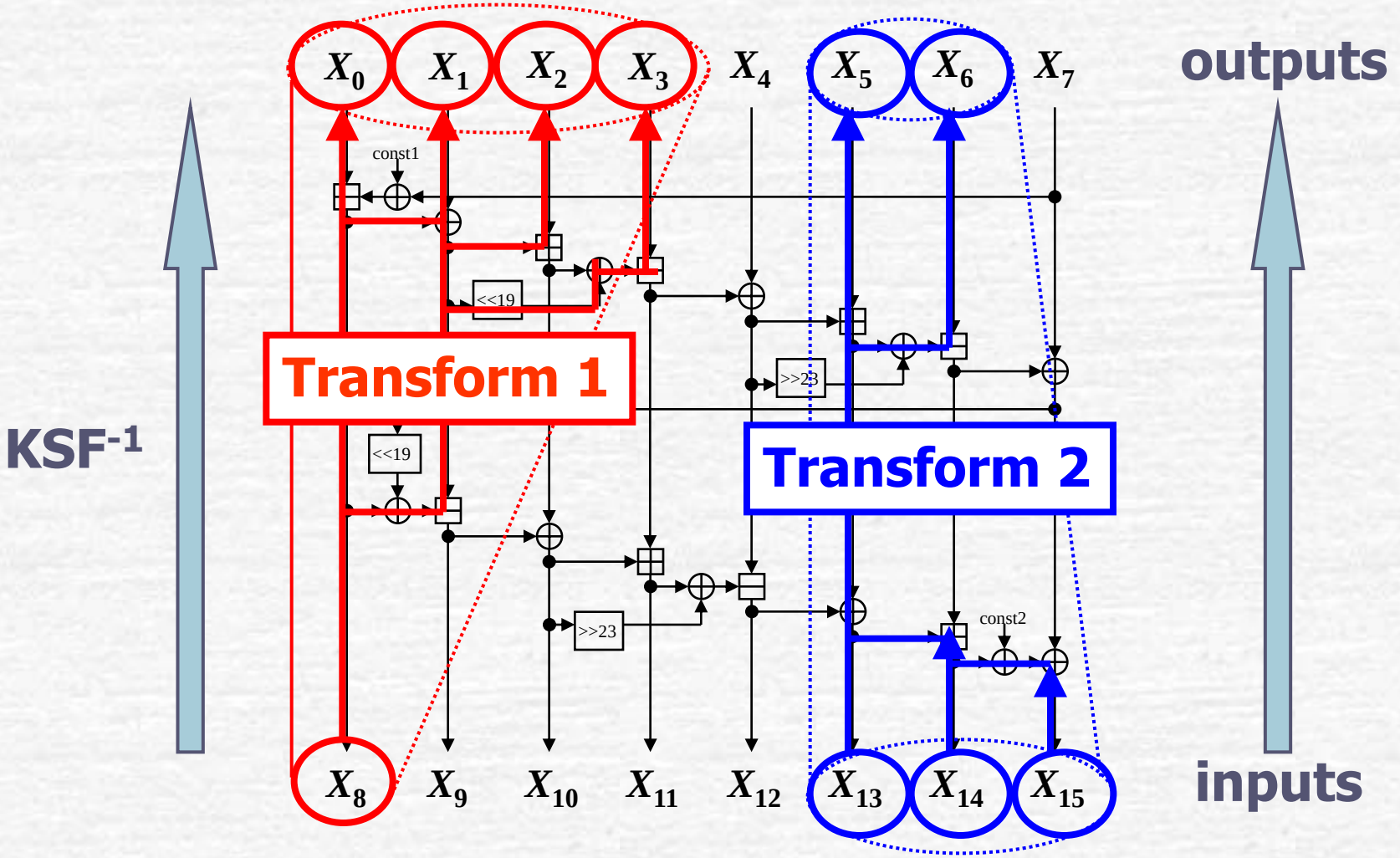
ΔX_{13}, ΔX_{14} and ΔX_{15} affect X_0, X_1, X_2, X_3 X_5, X_6, X_7

Transform 2

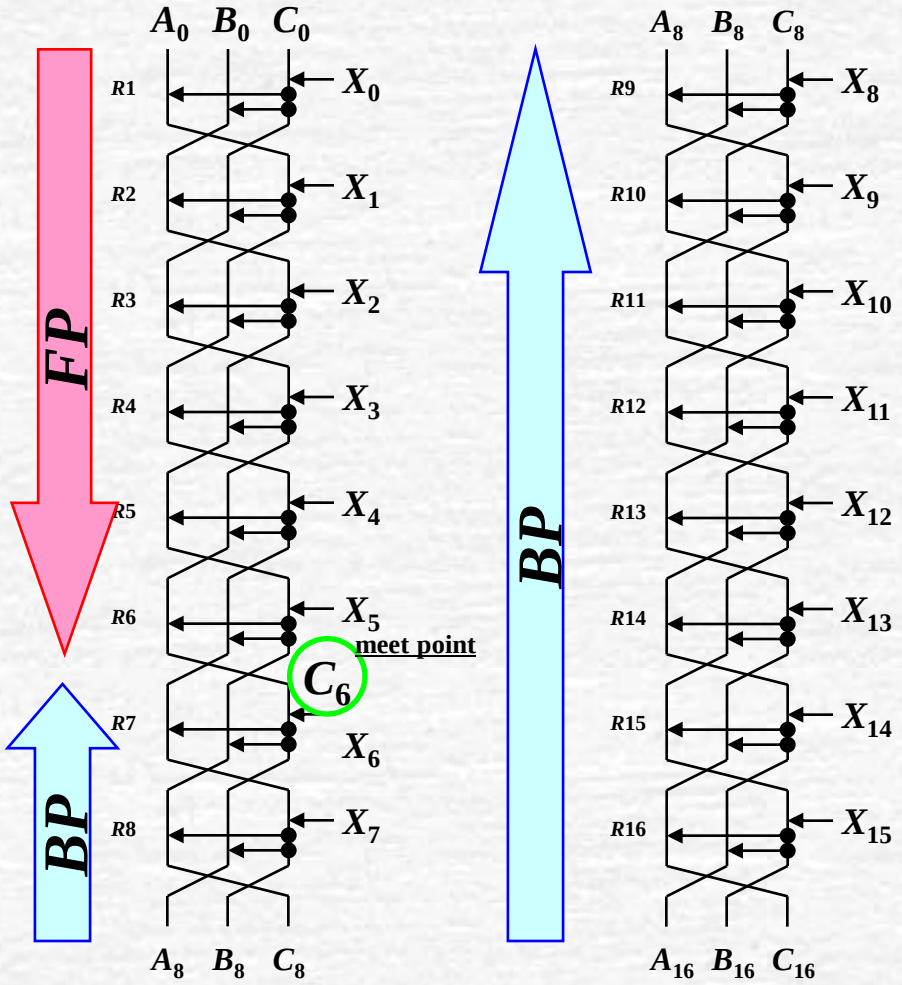


ΔX_{13}, ΔX_{14} and ΔX_{15} affect only X_5 and X_6

Independent Transforms in the KSF

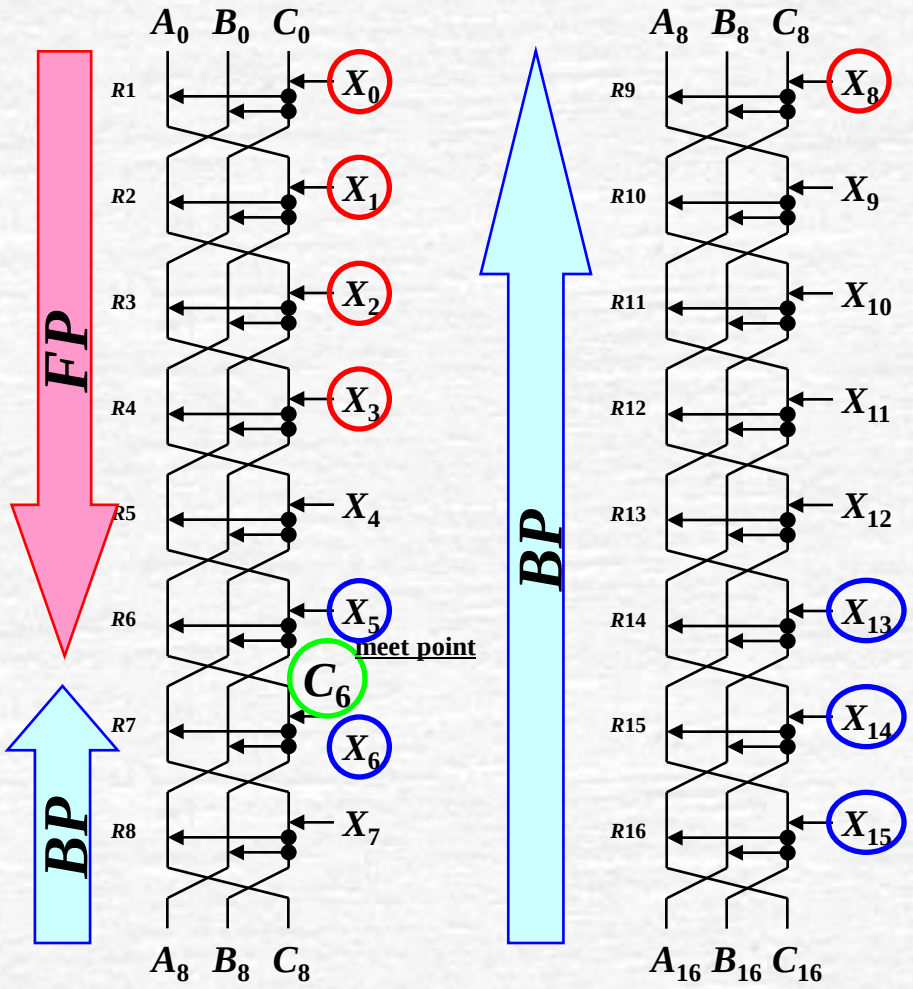


Preimage attack on 16-round Tiger



- **meet point** : C_6 (64 bits)
- **FP** : 1 – 6 rounds
  (Forward Process)
- **BP** : 7 – 16 rounds
  (Backward Process)

Preimage attack on 16-round Tiger

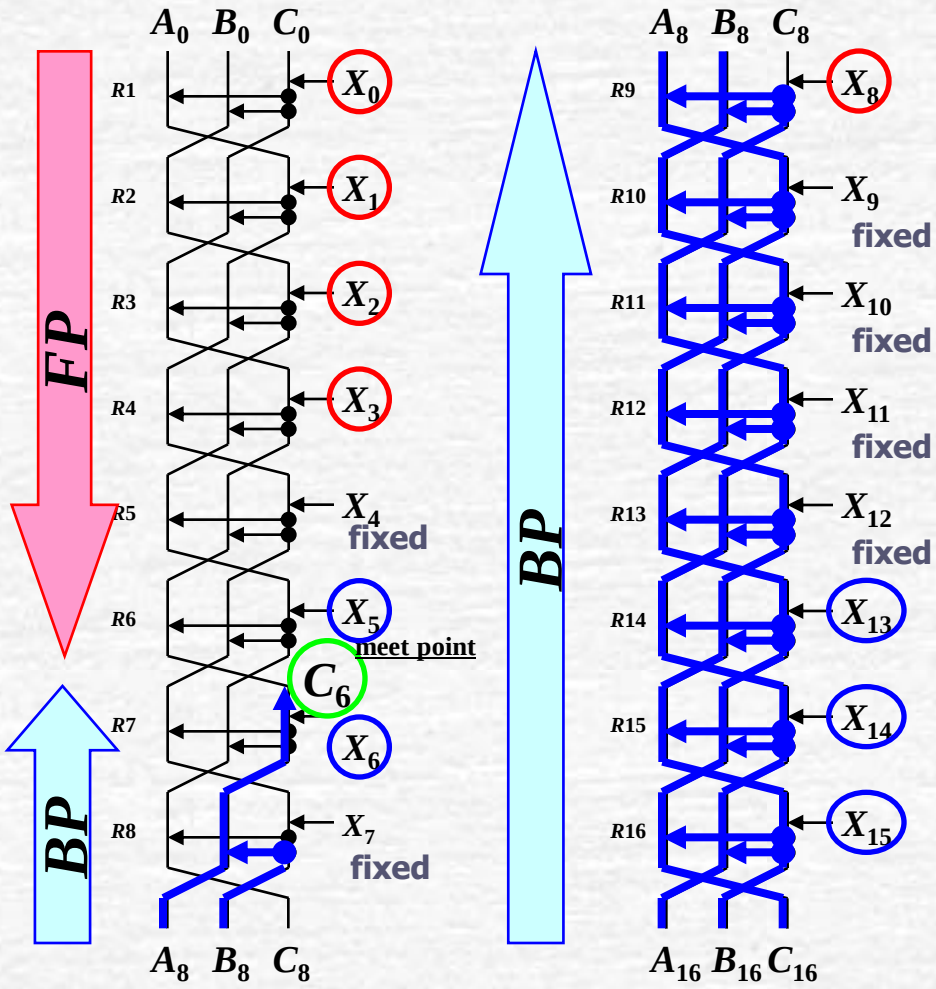


- **meet point** : C_6 (64 bits)
- **FP** : 1 – 6 rounds
  (Forward Process)
- **BP** : 7 – 16 rounds
  (Backward Process)

: variables of Transform 1

: variables of Transform 2

BP (Backward Process)



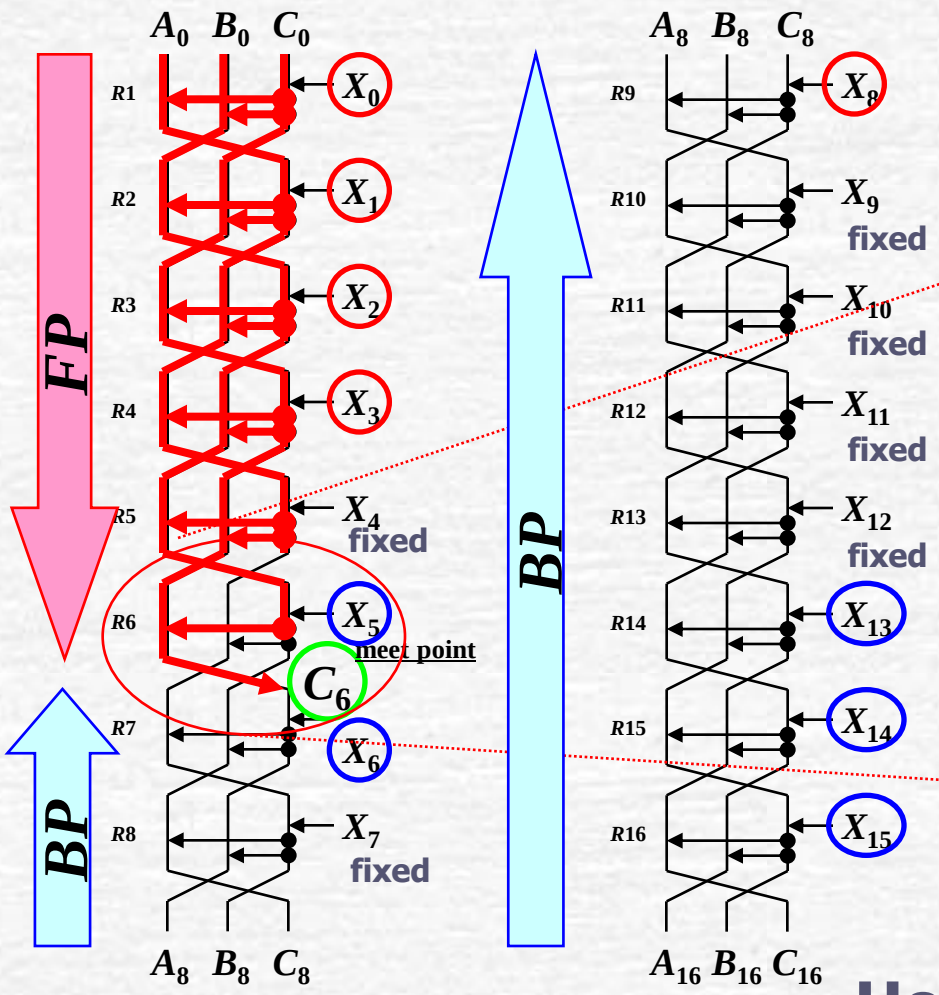
BP (Backward Process)

-Problem: X_8

X_8 is changed when X_0-X_3 are changed
But, C_6 can be calculated without X_8

Thus, X_8 can be ignored in the **BP**

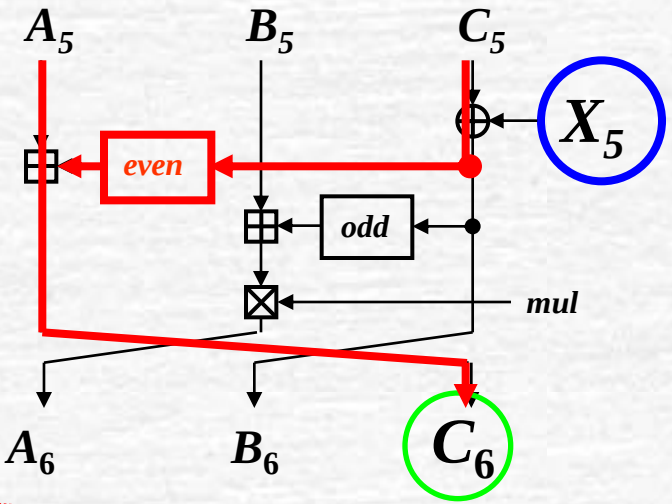
FP (Forward Process)



FP (Forward Process)

-Problem: X_5

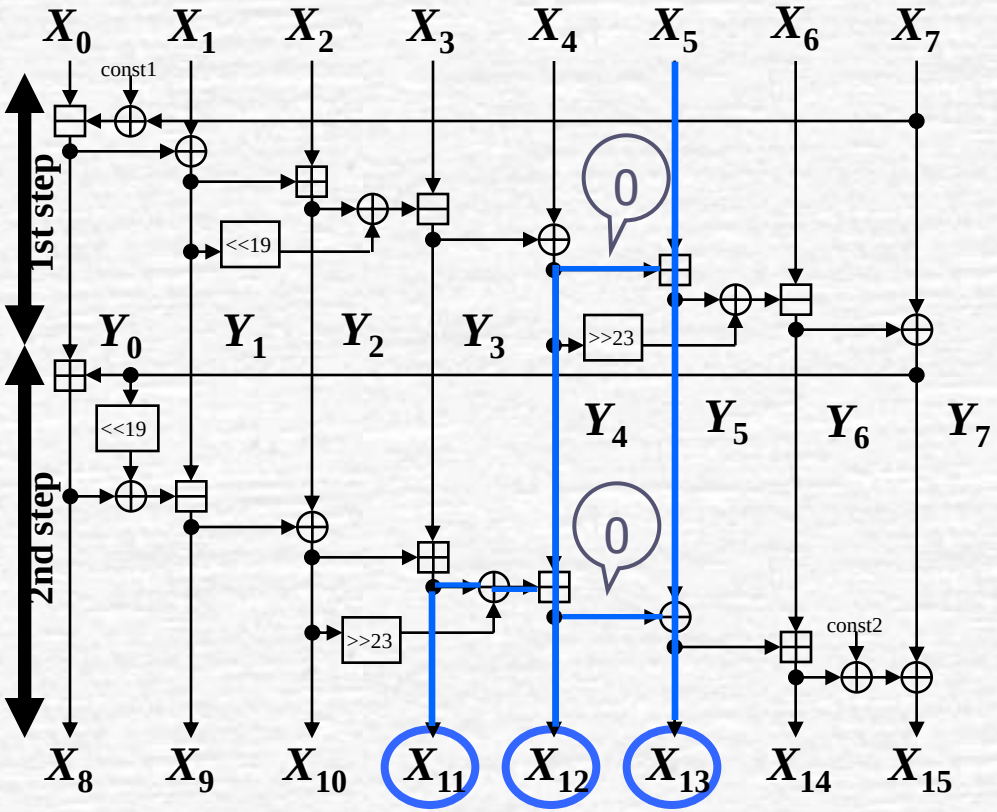
X_5 is changed when X_{13}-X_{15} are changed



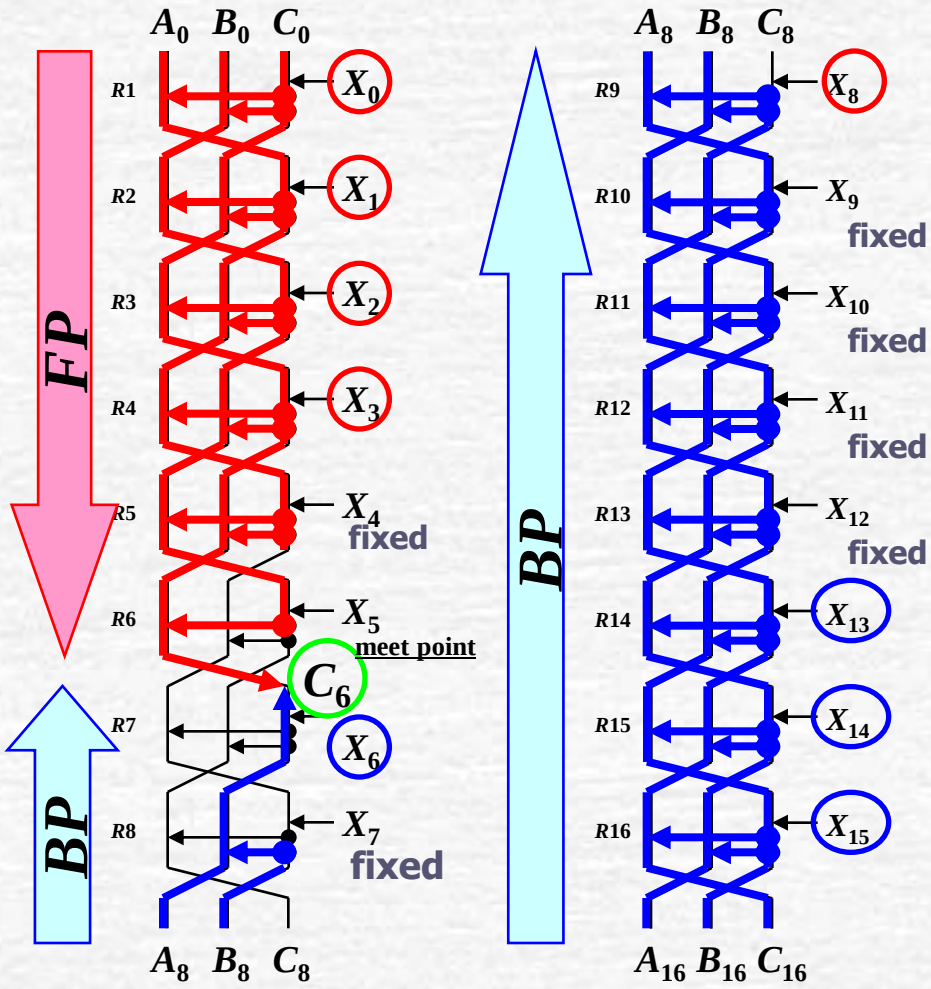
How to fix even bytes of X_5 ?

How to fix even bytes of X_5

- **Even bytes of X_5 can be fixed by choosing X_{11}, X_{12} and X_{13} properly.**
  - When X_{12} and Y_4 are zero, X_5 is identical to X_{13}.
    Thus, if even bytes of X_{13} are fixed, even bytes of X_5 are also fixed
  - Y_4 can be fixed to zero by choosing X_{11} as $X_{11} = X_{10} >> 23$



Preimage attack on 16-round Tiger



- We can execute FP and BP independently

We can succeed in applying MITM to 16-round Tiger!

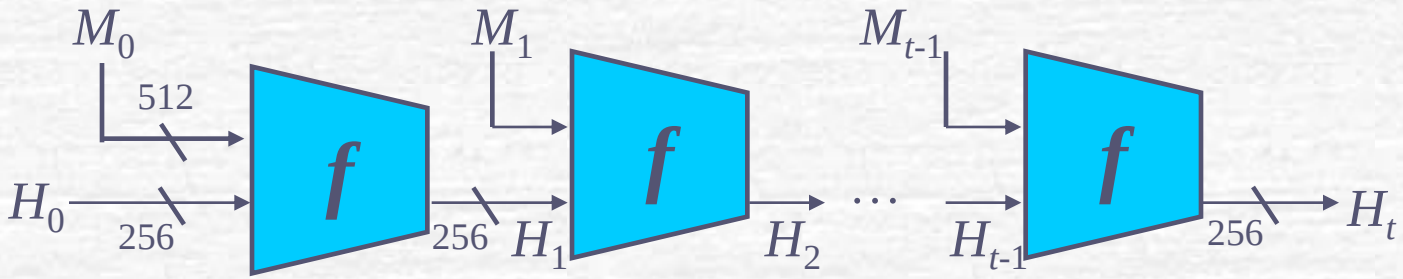
Evaluation

Meet point : C_6 (64 bits), $l = 64$
Complexity : $2^{n-l/2} = 2^{192 - 64/2} = 2^{160}$
Memory : $2^{35.6}$ bytes (2^{32} x 96 bits)

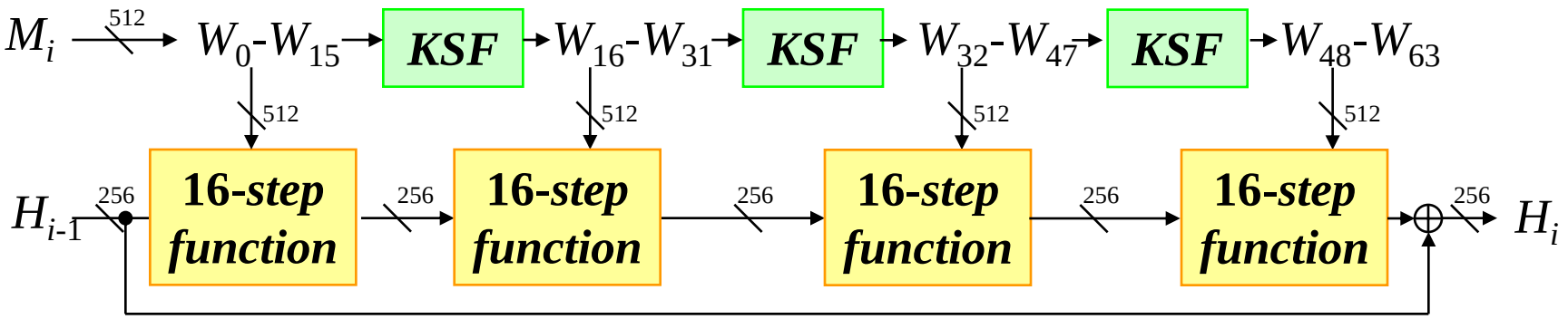
- IV words A_0, B_0, C_0, and padding word X_7 can be controlled
  => easy to extend to **"one-block"** preimage attack !
  (Complexity = 2^{161}, since 1 padding bit cannot be controlled)
- Also, easy to extend to "one-block" 2nd preimage attack !
  (Our preimage attack can obtain random preimages from a target)

SHA-256 hash function

- **SHA-256 hash function**

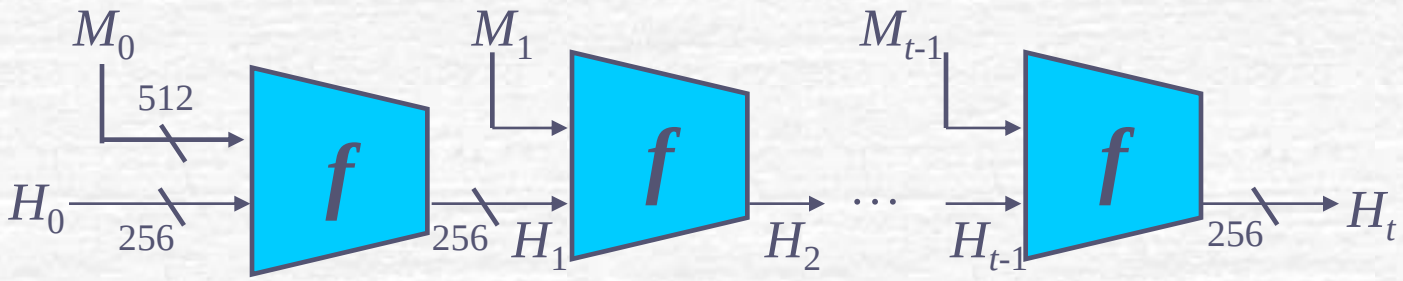


- **Compression function *f* (64 steps)**

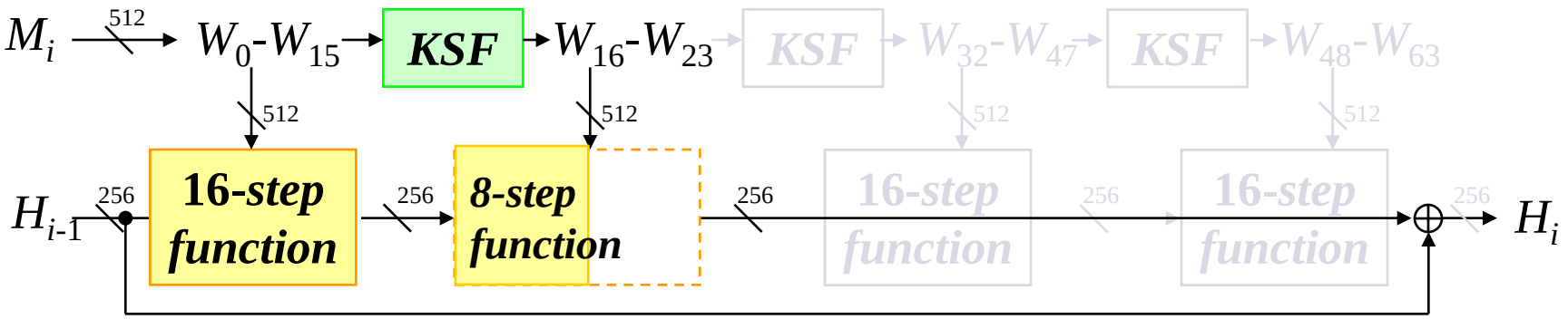


SHA-256 hash function

- **SHA-256 hash function**

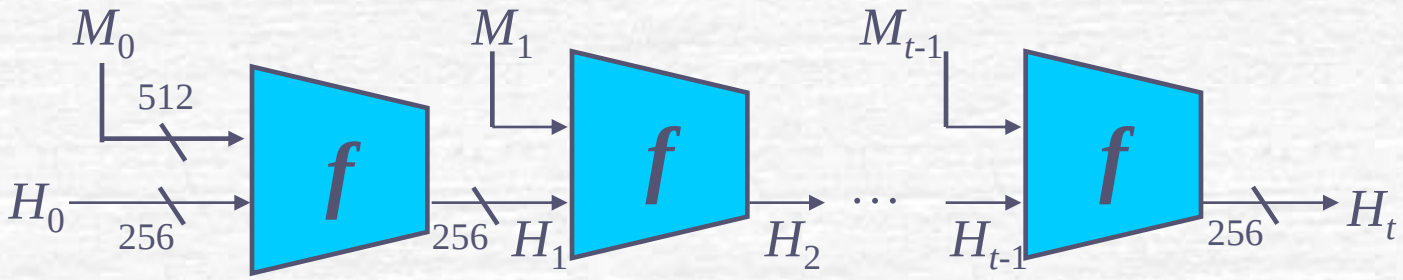


- **Compression function *f* (64 steps -> 24 steps)**

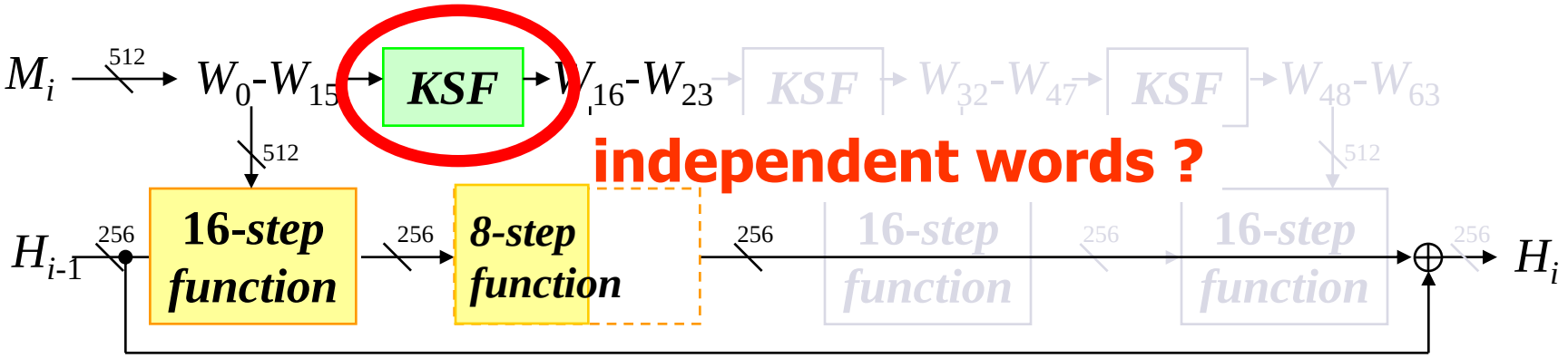


SHA-256 hash function

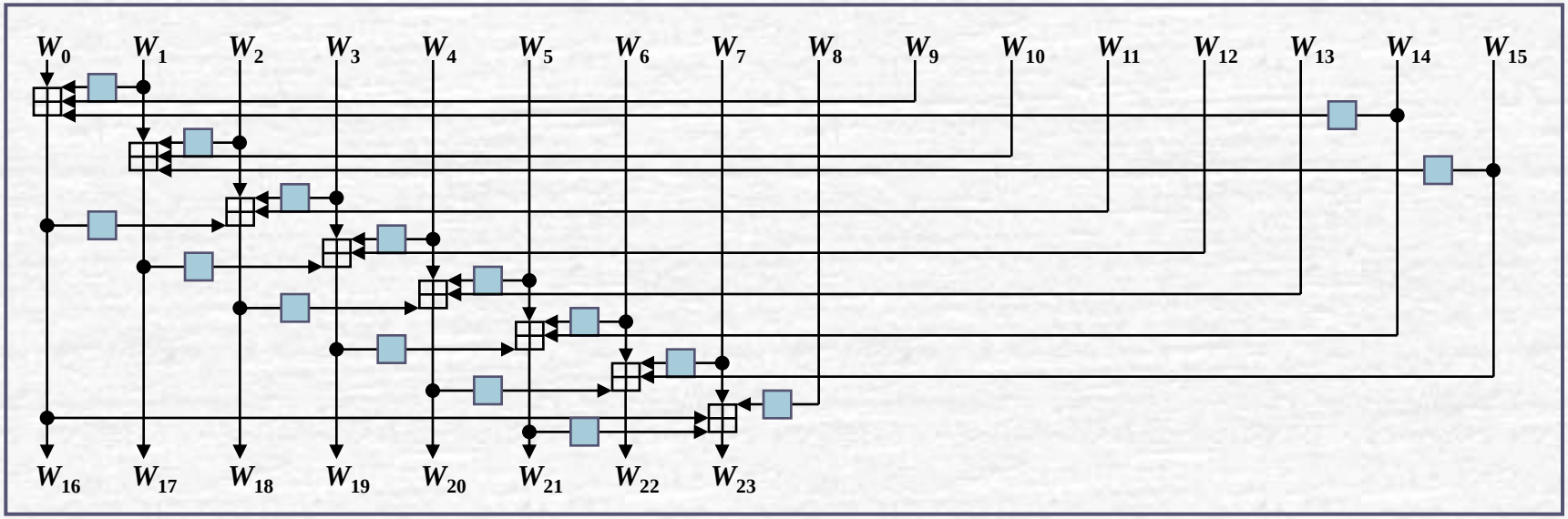
- SHA-256 hash function



- Compression function f (64 steps -> 24 steps)

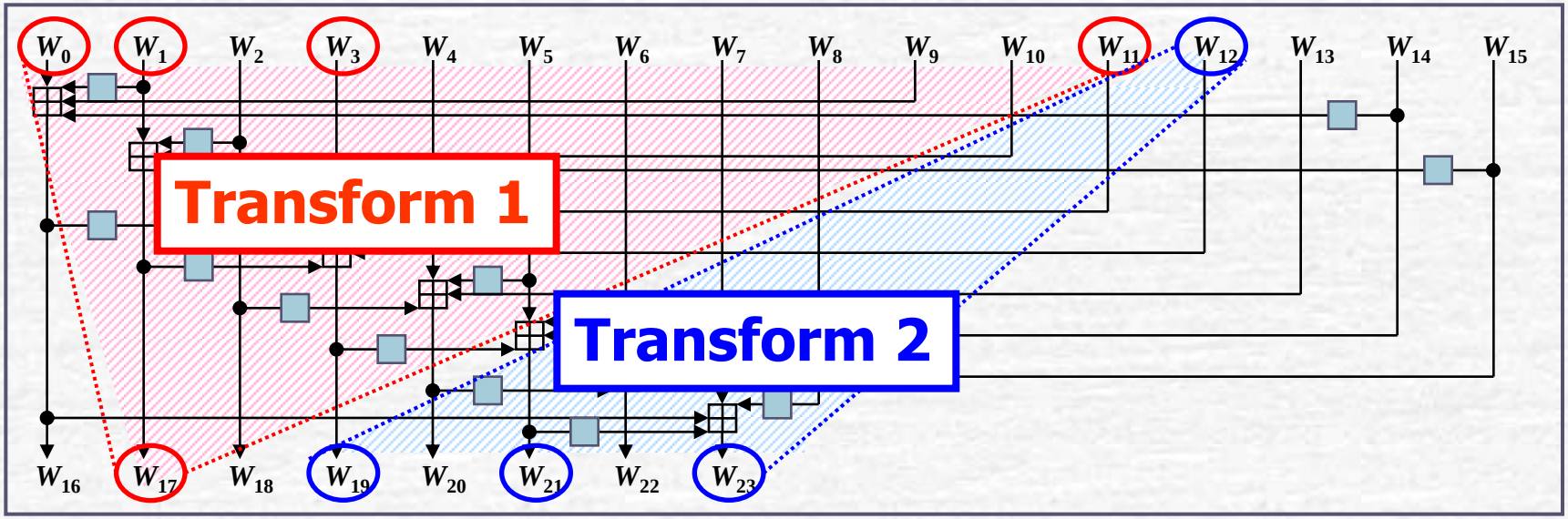


Independent transforms in the KSF



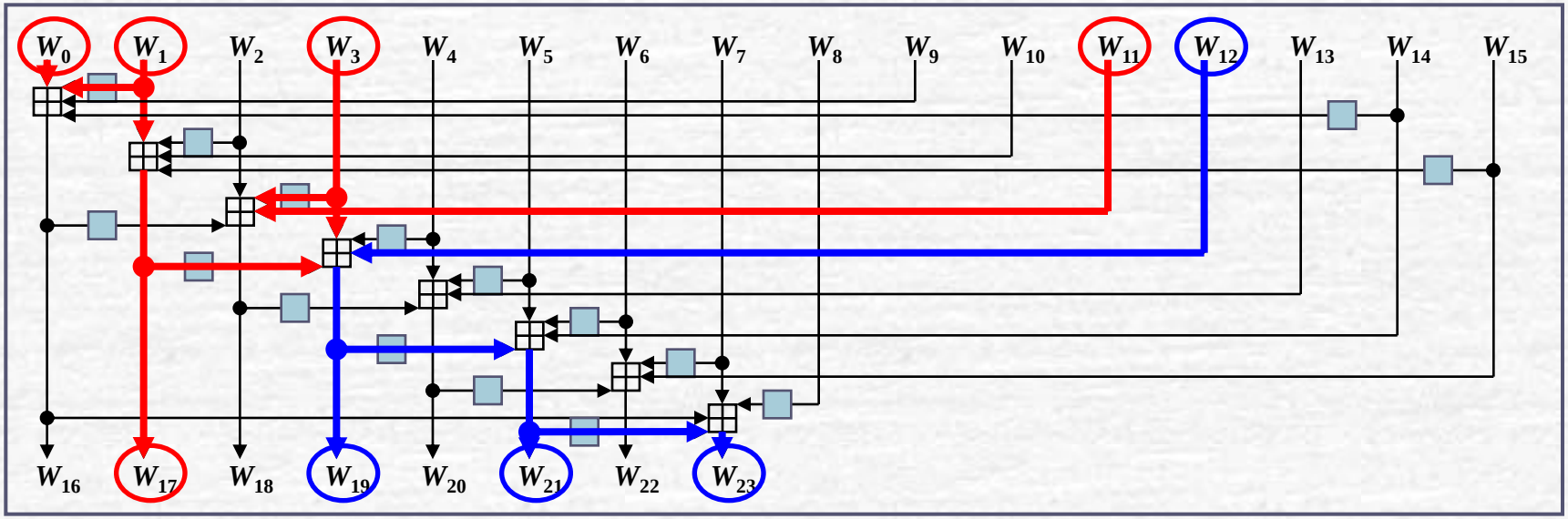
$$W_i = \begin{cases} m_i & (0 \leqq i \leqq 15) \\ \sigma_1(W_i - 2) + (W_i - 7) + \sigma_0(W_i - 15) + W_i - 16 & (16 \leqq i \leqq 24) \end{cases}$$

Independent transforms in the KSF



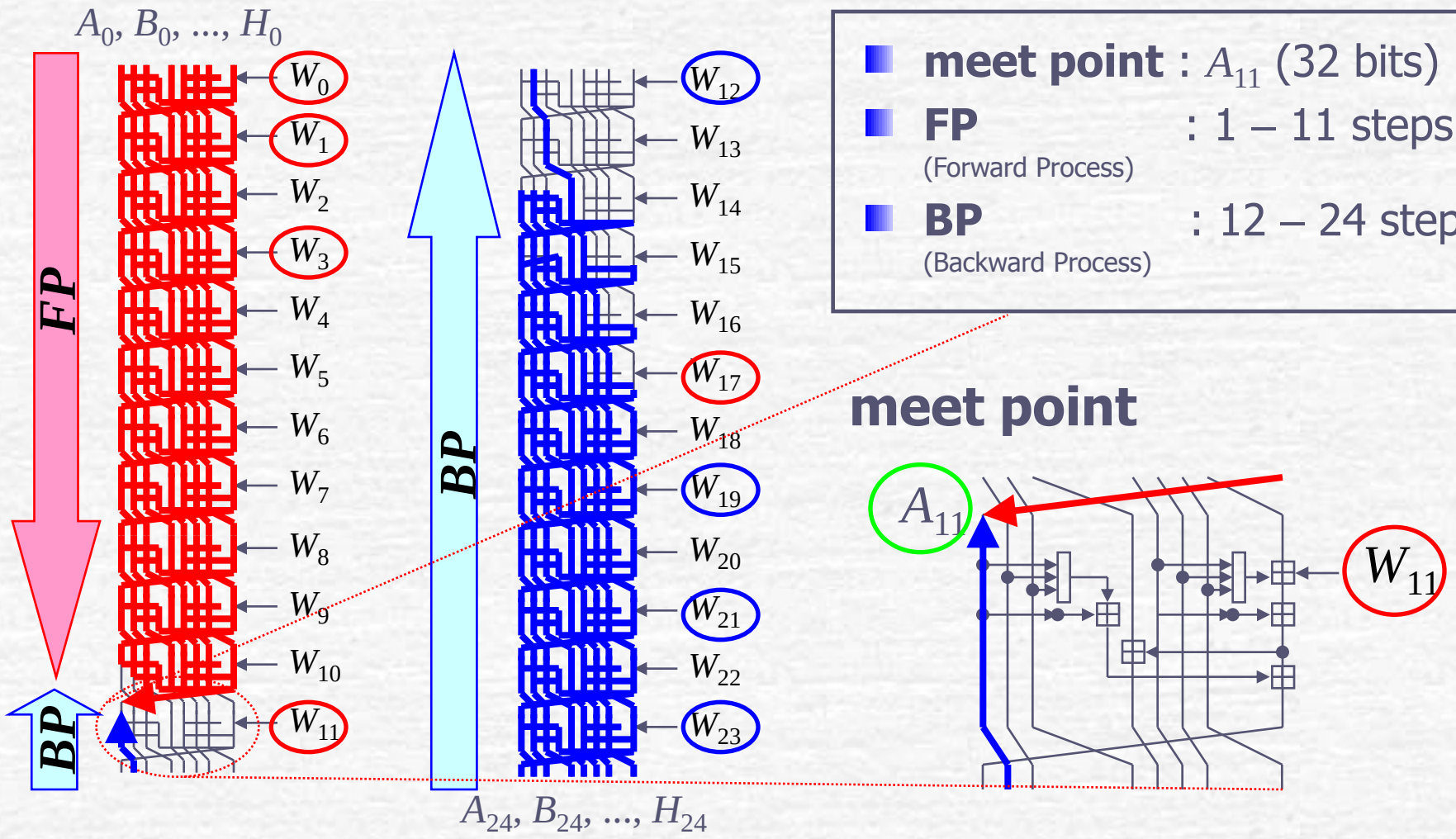
$$W_i = \begin{cases} m_i & (0 \leqq i \leqq 15) \\ \sigma_1(W_i - 2) + (W_i - 7) + \sigma_0(W_i - 15) + W_i - 16 & \\ & (16 \leqq i \leqq 24) \end{cases}$$

Independent transforms in the KSF



$$W_i = \begin{cases} m_i & (0 \leqq i \leqq 15) \\ \sigma_1(W_i - 2) + (W_i - 7) + \sigma_0(W_i - 15) + W_i - 16 & (16 \leqq i \leqq 24) \end{cases}$$

Preimage attack on 24-step SHA-256



- **meet point** : A_{11} (32 bits)
- **FP** : 1 – 11 steps
  (Forward Process)
- **BP** : 12 – 24 steps
  (Backward Process)

Evaluation

Meet point : A_{11} (32 bits), $l = 32$
Complexity : $2^{n-l/2} = 2^{256 - 32/2} = 2^{240}$
Memory : 2^{19} bytes (2^{16} x 64 bits)

- IV words A_0, …, H_0, and padding words W_{14}, W_{15} can be controlled
  easy to extend to **"one-block"** preimage attack
  (attack complexity = 2^{240})
- Also, easy to extend to "one-block" 2nd preimage attack
- This attack can be extended to the SHA-512
  - **The complexity of (2 nd) preimage attack of SHA-512 is 2^{480}**
    because meet point is 64 bits.

Conclusion

- **We proposed 1-block preimage attacks on 16-round Tiger and 24-step SHA-2**
  - **These attacks are based on the meet-in-the-middle attack.**

We developed techniques to find "independent words" by using "independent transforms" .

To use independent transform for MITM, we utilize relation between messages and internal variables.

Even if KSF is more complicate than MD4 and MD5, MITM preimage attack can apply to it by using our techniques!!

Thank you for your attention !