Meet-in-the-Middle Preimage Attacks on AES Hashing Modes and an Application to Whirlpool

Yu Sasaki

NTT Corporation

NTT

Summary

- Preimage attacks on AES hashing modes.
- Achieve best attacks in terms of the classical security notions of hash functions.

Attack	Rounds	Modes	Time	Mem.	Ref.
Collision	6	MMO, MP	2^{56}	2^{32}	[LM+09]
2nd Pre.	7	MMO, MP	2^{120}	2^{8}	New!!
Preimage	7	DM	2^{125}	2^{8}	New!!
Distinguish	8	MMO, MP	2^{48}	2^{32}	[GP10]

(the same results for all size keys)

DM: *Davies-Meyer*, **MMO**: *Matyas-Meyer-Oseas*,
MP: *Miyaguchi-Preneel*

NTT

Outline

- Motivation
- Problems of current techniques
- Our attacks
- Application to Whirlpool

NTT

Motivation (Industry)

- Block-ciphers offer various facilities through mode-of-operations; Hash, MAC, Stream-cipher
- When we need block-ciphers and hash functions in a constrained environment, we only implement a block-cipher and build a hash function with it.
- Small digest size is used in such an environment. e.g. 80-bit and 64-bit hash functions [CHES08]
- AES hashing modes are possible candidates!

Motivation (Academic)

- Previous analyses on AES hash usage considered differential properties.

  Ex. - Known-key attack on 8-round AES

  - Differential attack on Whirlpool, ECHO, and Grøstl

Question

How does AES-hash resist preimage attacks?

- Our attack is MitM attack, which works efficiently for hash function with weak message schedule.

Question

How can it be applied for dedicated block-ciphers with complicated key schedule algorithm?

NTT

Practical Security Criteria

- Current cryptanalyses are often very theoretic.

  Ex. - Related-subkey attack on block-ciphers

  - Non-ideal property of compression functions

- Recently, security in a more practical scenario has been evaluated.

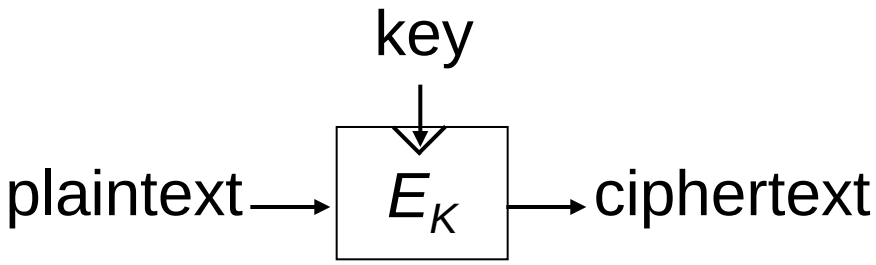
  Ex. - Single-key attack on AES and GOST

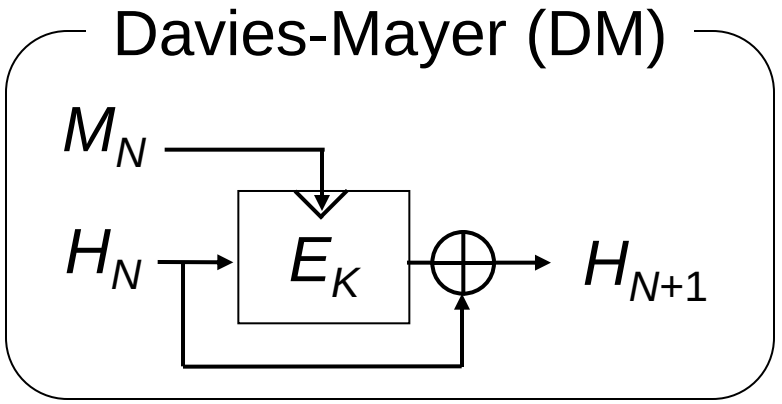
  - Security as hash function in SHA-3

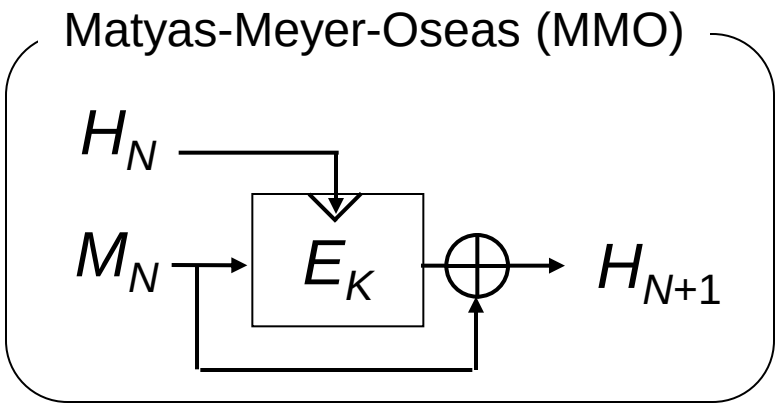
- In this research, we evaluate classical security notions of hash functions. (preimage resistance)

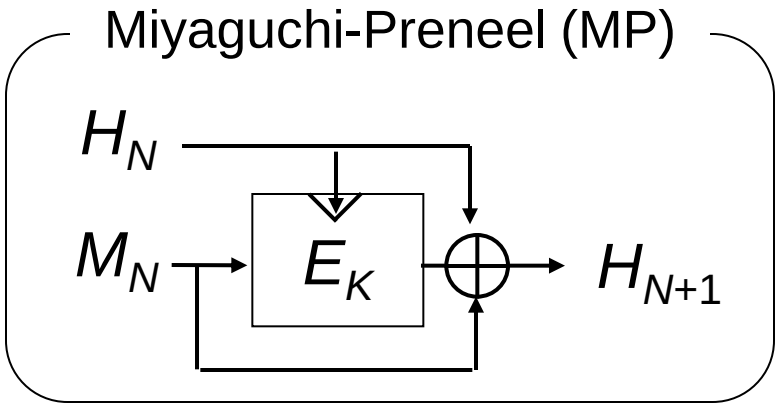
Hashing Modes in Block-Ciphers

- PGV construction is a synthetic approach.
- The followings are used in practice.









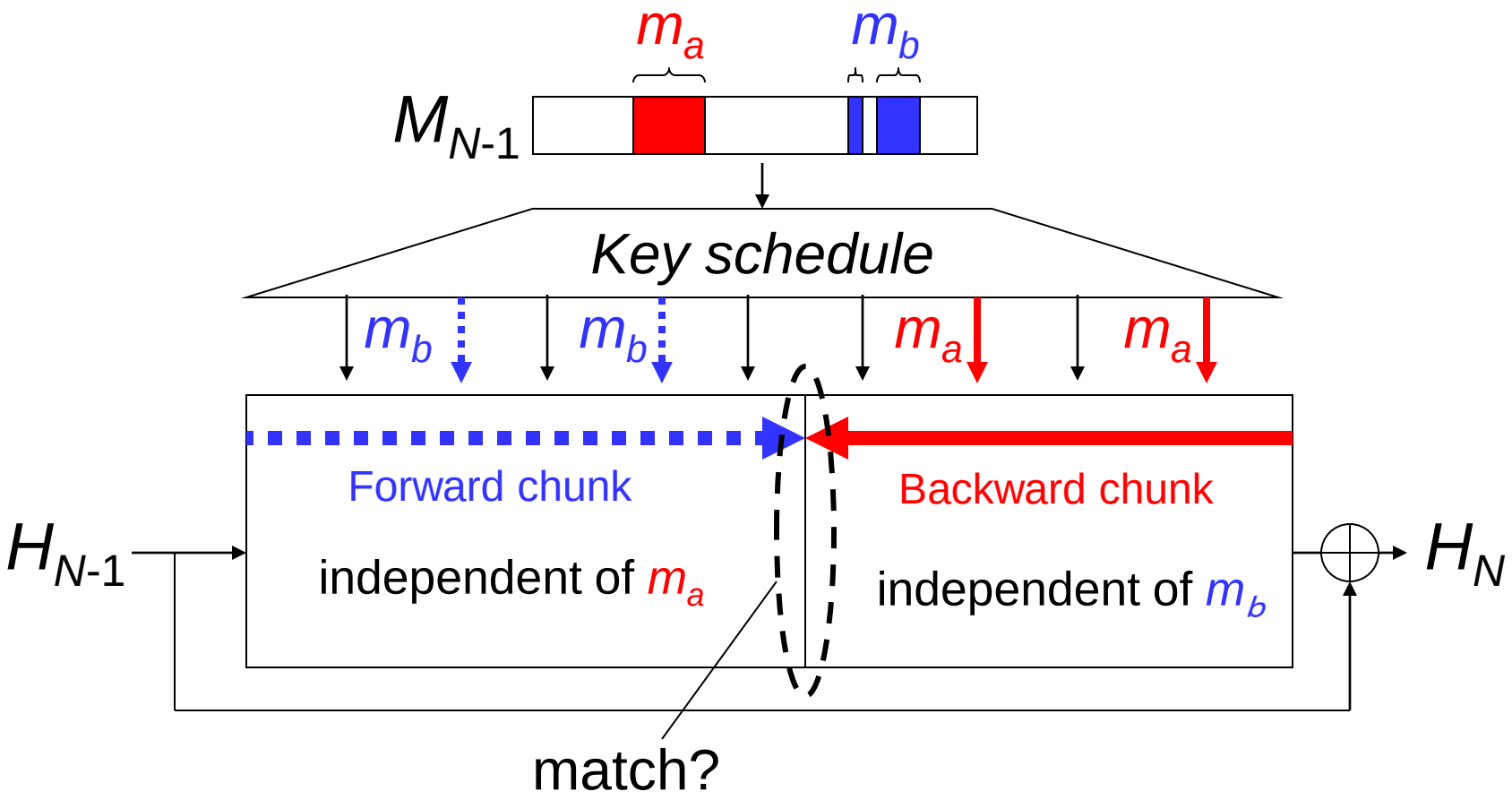
NTT

Outline

- Motivation
- Problems of current techniques
- Our attacks
- Application to Whirlpool

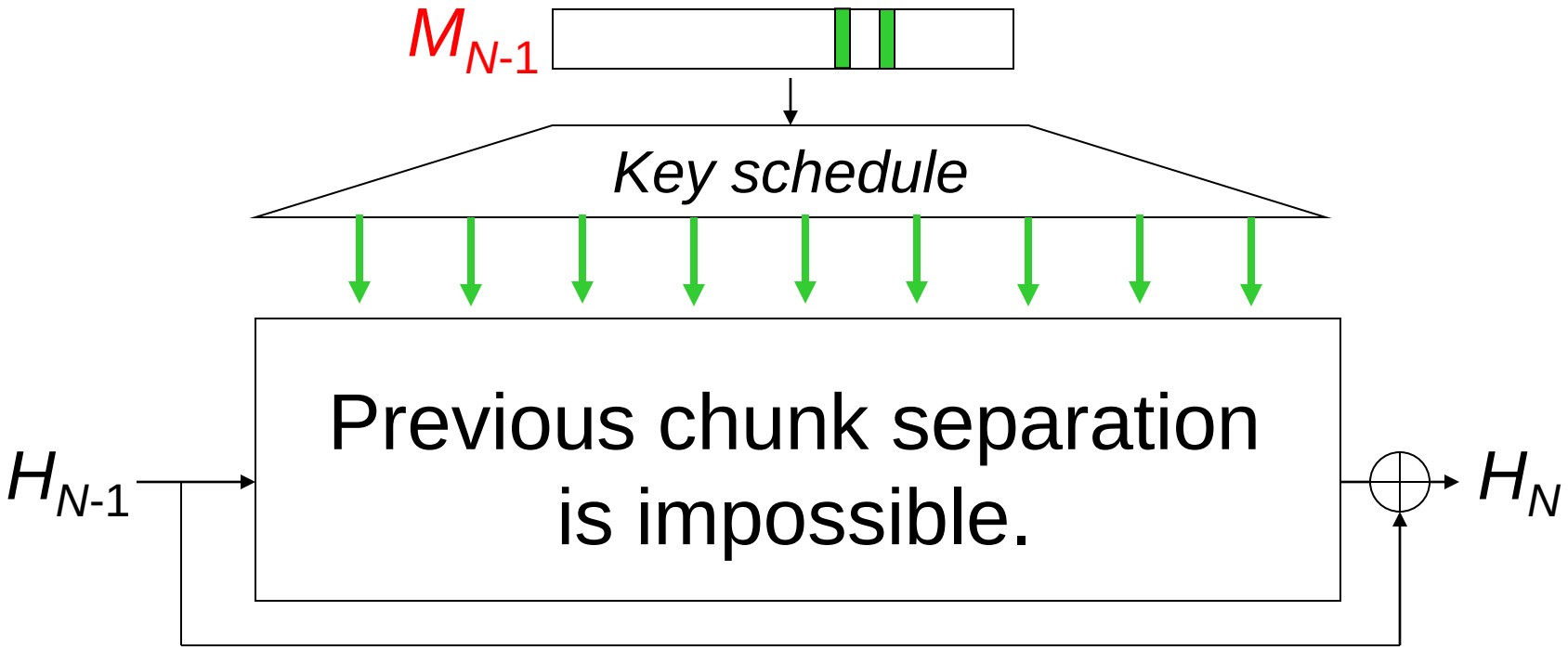
Meet-in-the-Middle Preimage Attack

Find message bits (words) which only impacts on a part of subkeys.



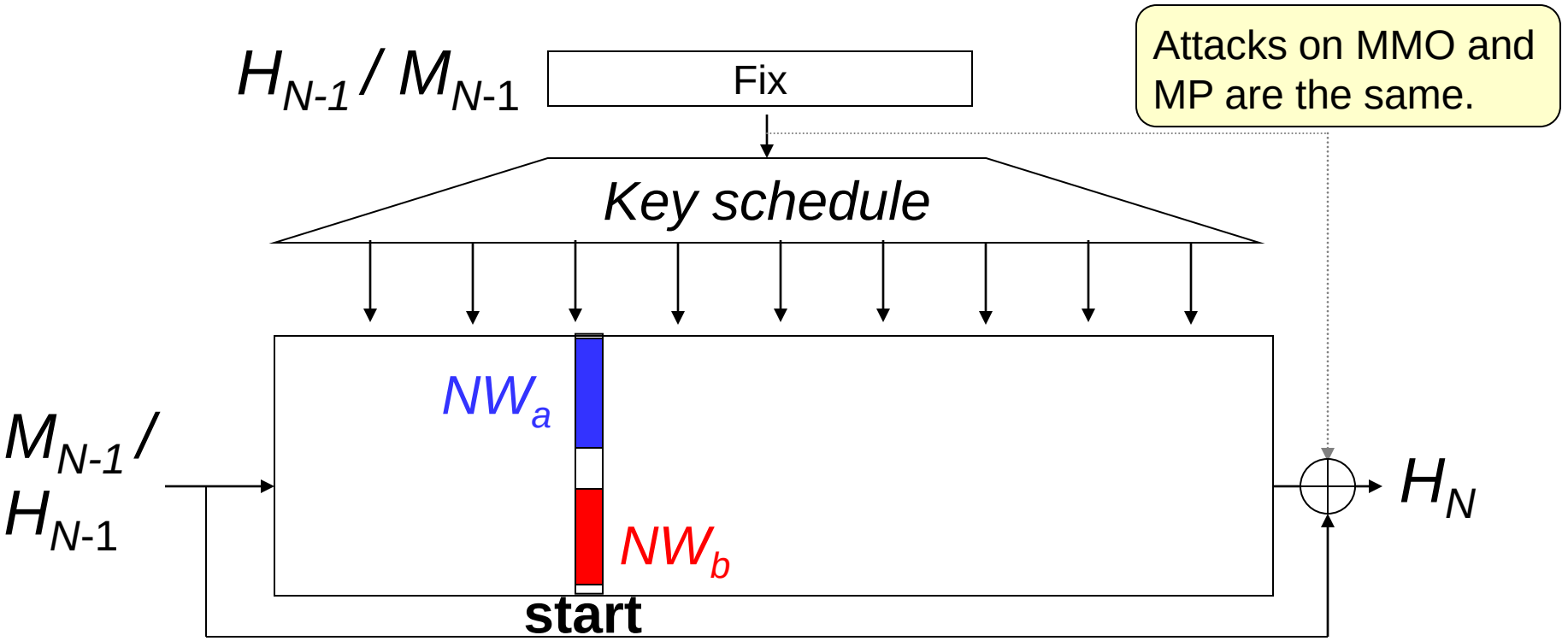
Problems for DM-AES

AES key schedule is bijective. Flipping any bit in a subkey will affect all other subkeys.



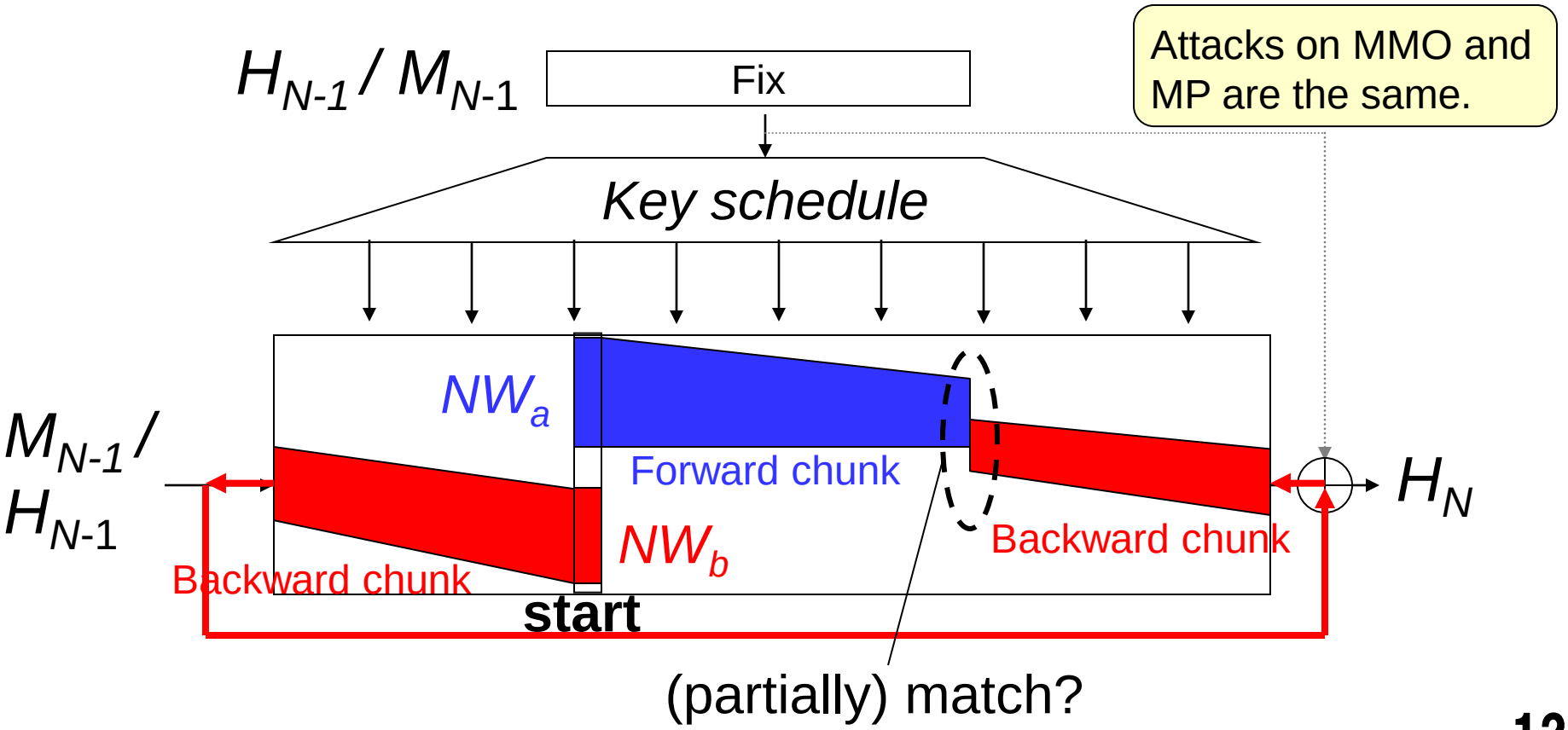
Our Idea

Fix the key, and use a part of internal state as neutral words.



Our Idea

Fix the key, and use a part of internal state as neutral words.



NTT

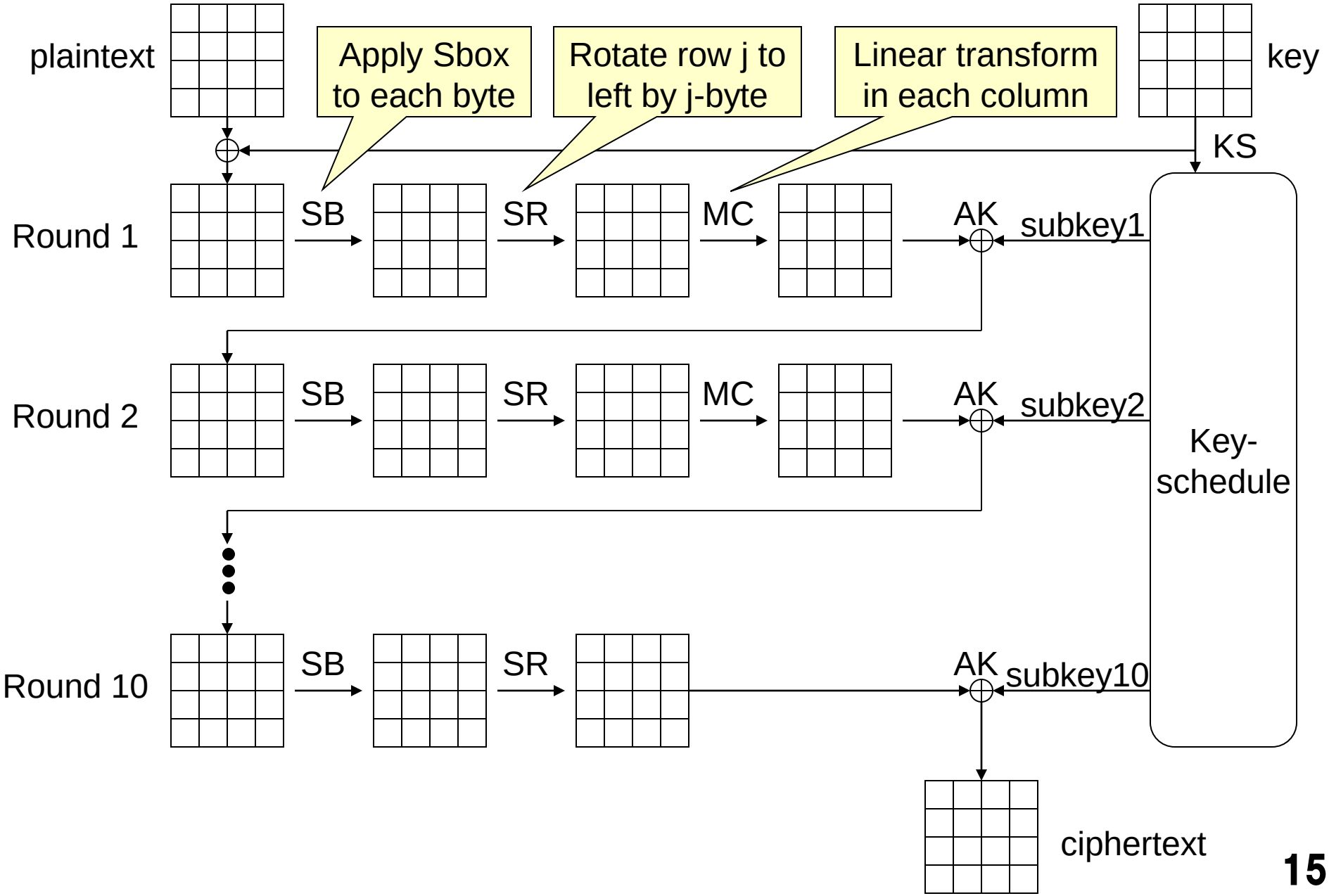
Outline

- Motivation
- Problems of current techniques
- Our attacks
- Application to Whirlpool

NTT

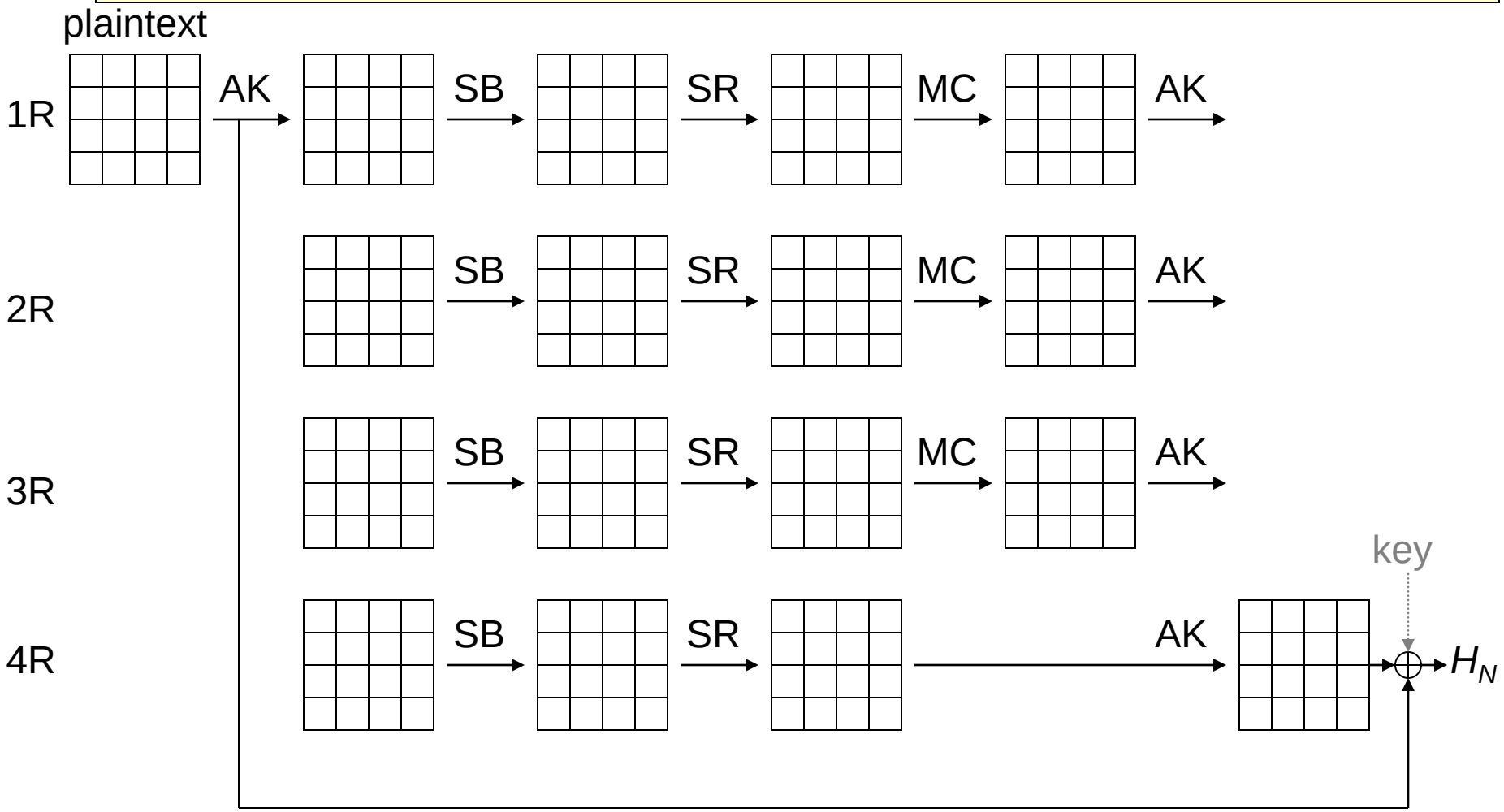
4-round attack

AES

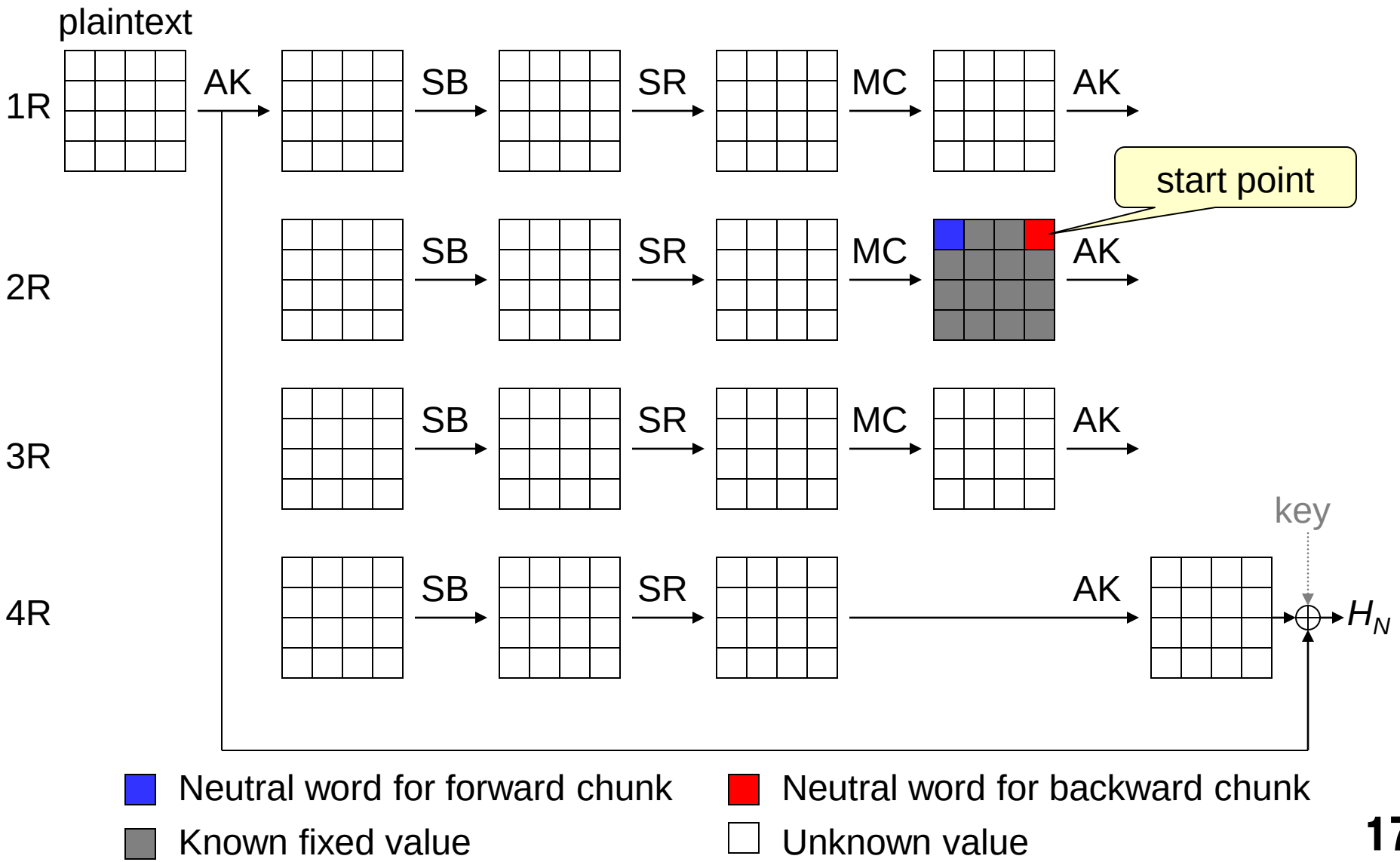

plaintext
Apply Sbox to each byte
Rotate row j to left by j-byte
Linear transform in each column
key
KS
Round 1
SB
SR
MC
AK
subkey1
Round 2
SB
SR
MC
AK
subkey2
Key-schedule
Round 10
SB
SR
AK
subkey10
ciphertext

Basic Attack (4-Round)

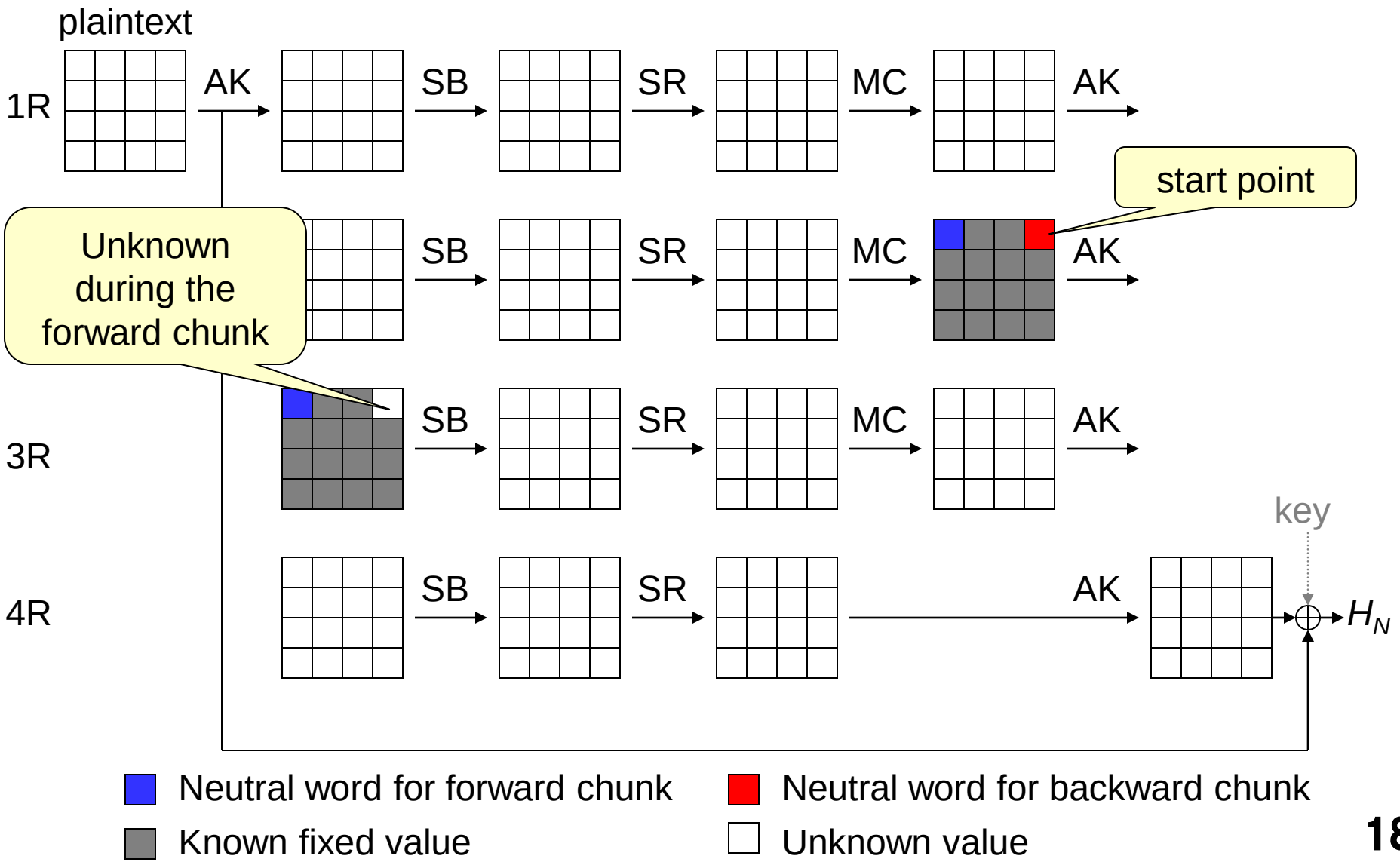
Generate pseudo-preimages → Convert to preimages or 2nd preimages (depends on modes)



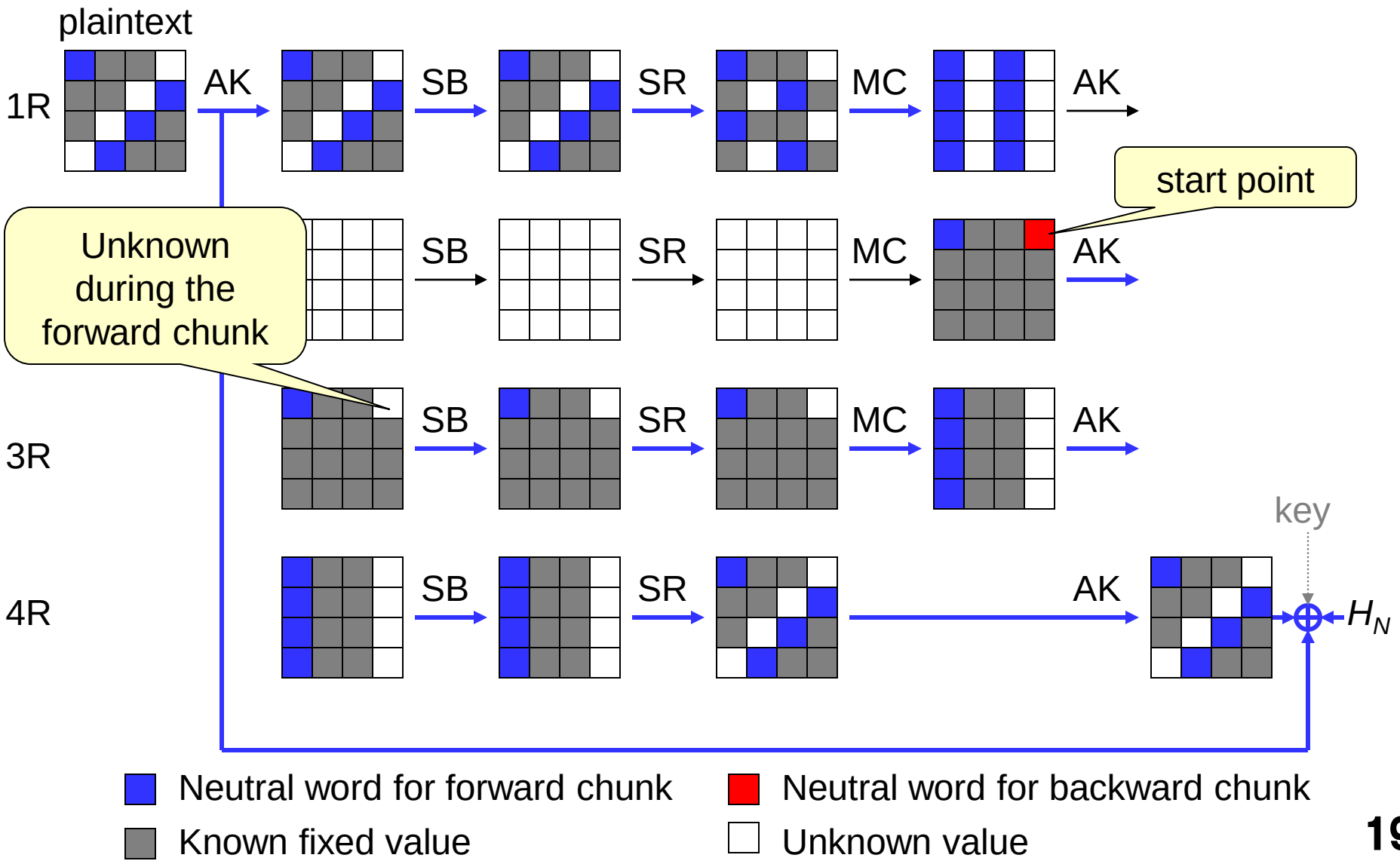
Basic Attack (4-round)



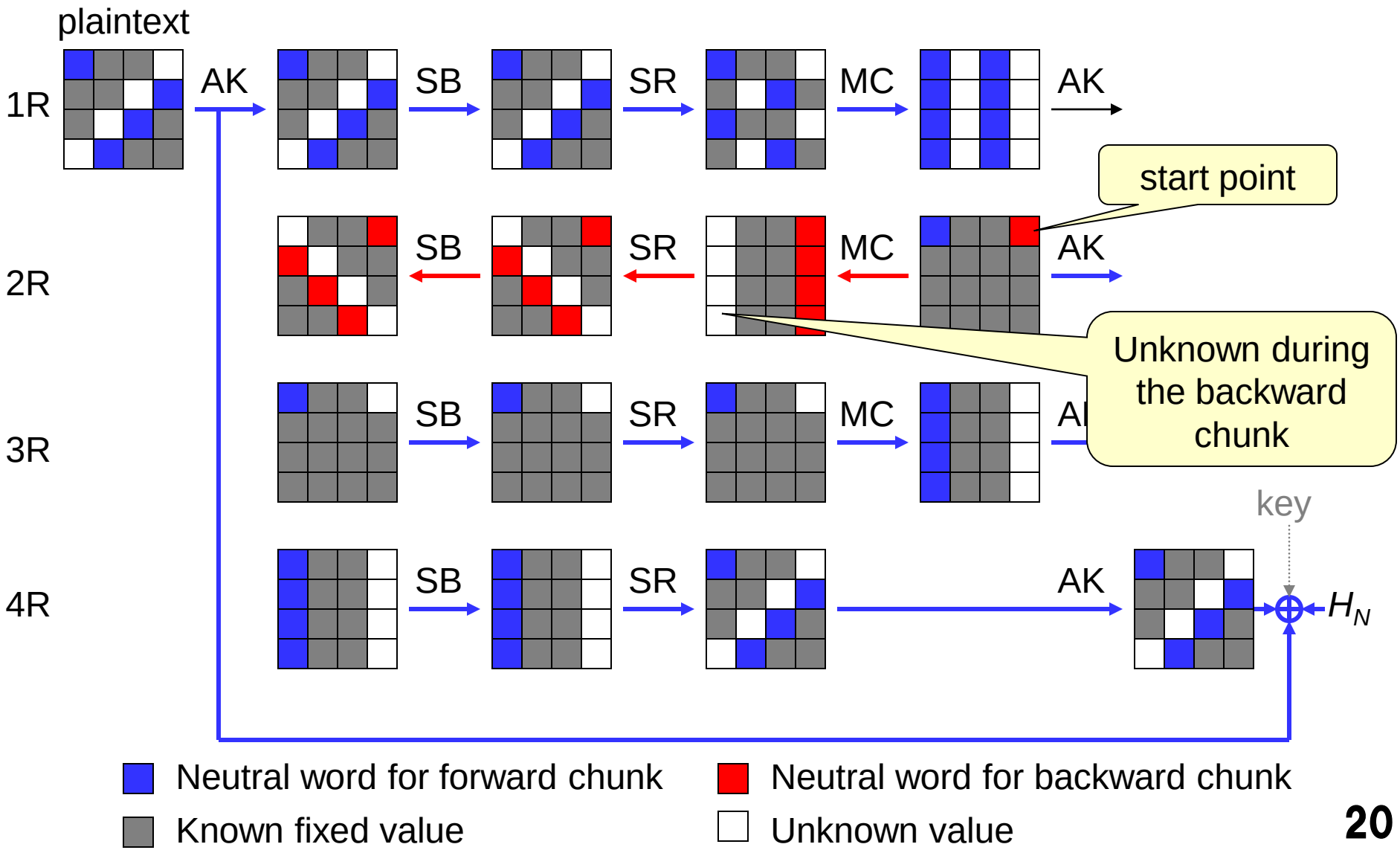
Basic Attack (Forward chunk)



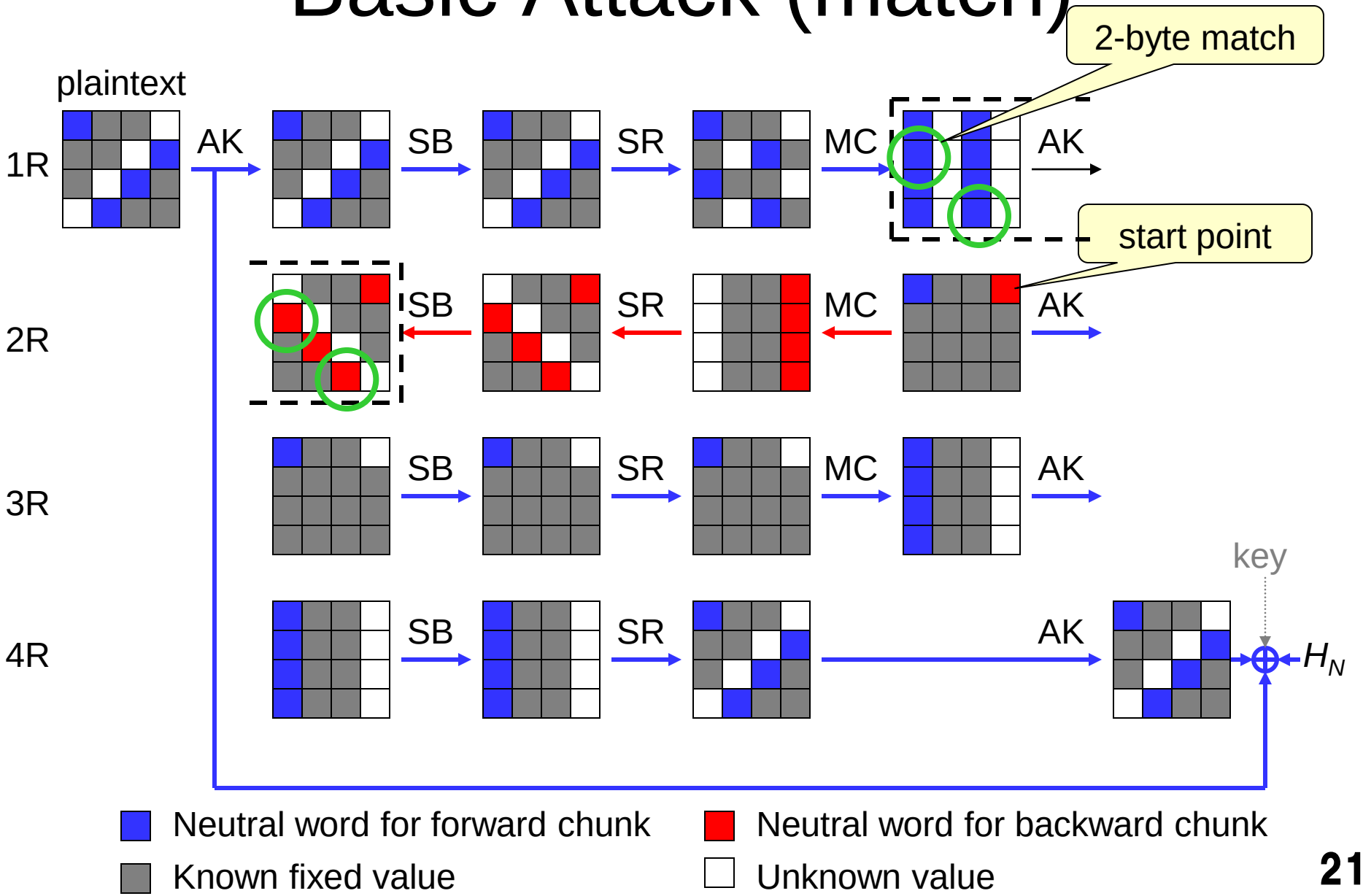
Basic Attack (Forward chunk)



Basic Attack (Backward chunk)



Basic Attack (match)



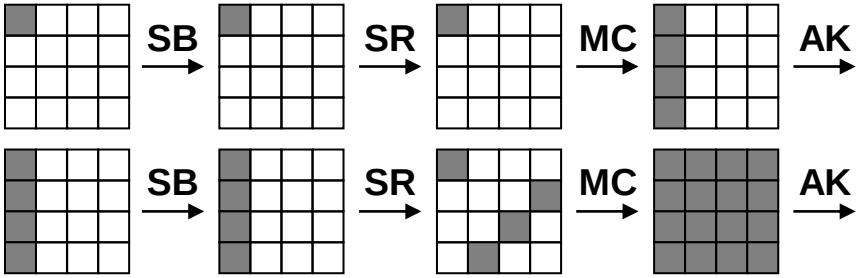
Summary of Basic Attack

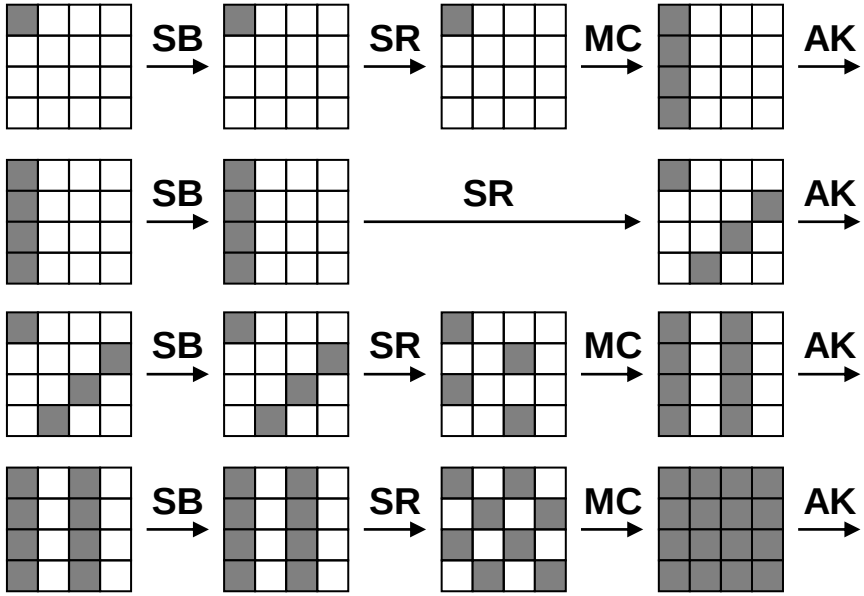
- Freedom degrees in forward is 8-bits.
- Freedom degrees in backward is 8-bits.
- 2-byte (=16-bit) match

- Pseudo-preimages are found faster than brute force attack by a factor of 2^8 ($=2^{120}$).

Observation

- The omission of MC in the last round is not related to the security of block-ciphers.
- However, in a hash function, the attackers can access to the internal state.



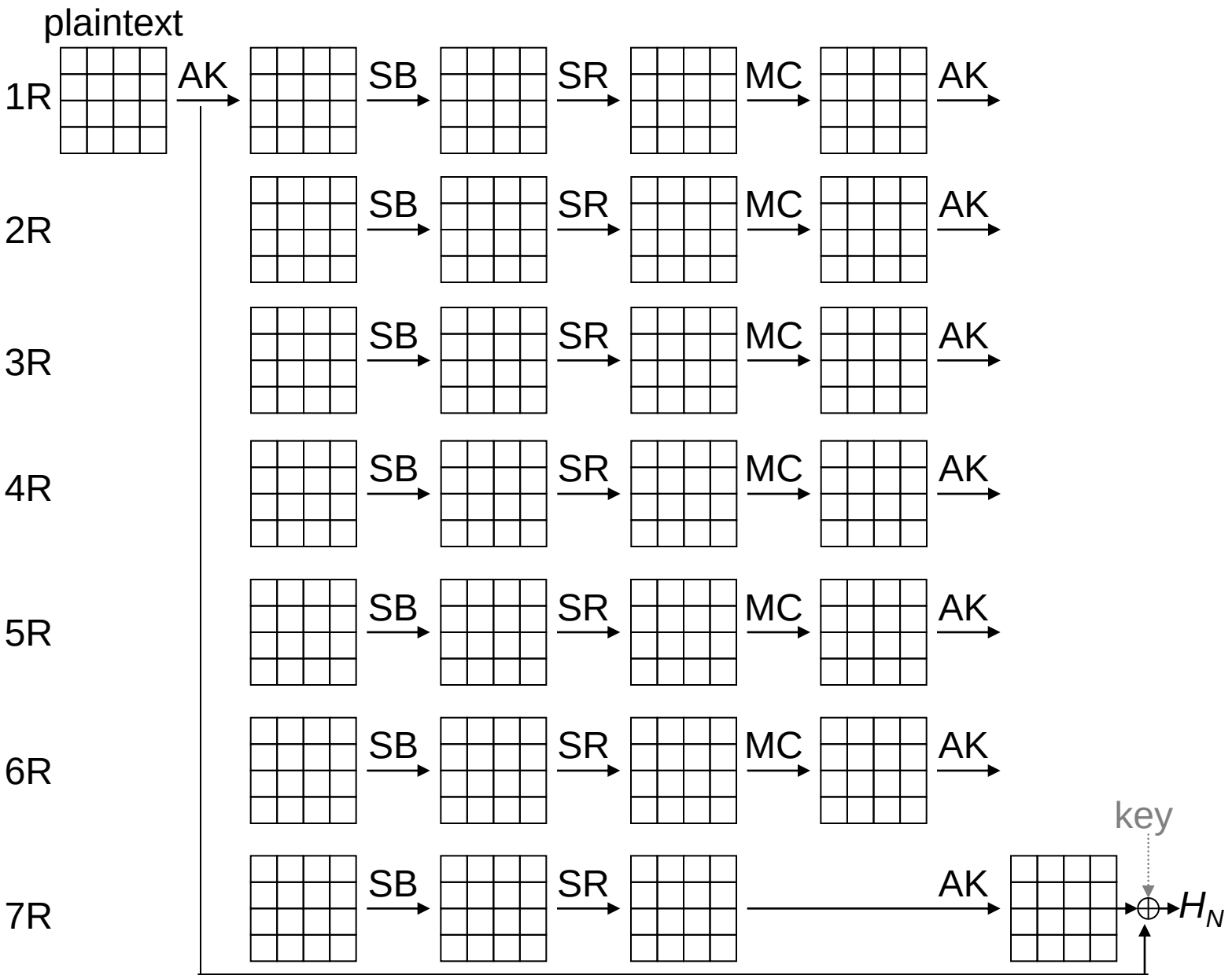


- If an attack starts from the second last round, 4 rounds are necessary to achieve the full diffusion.

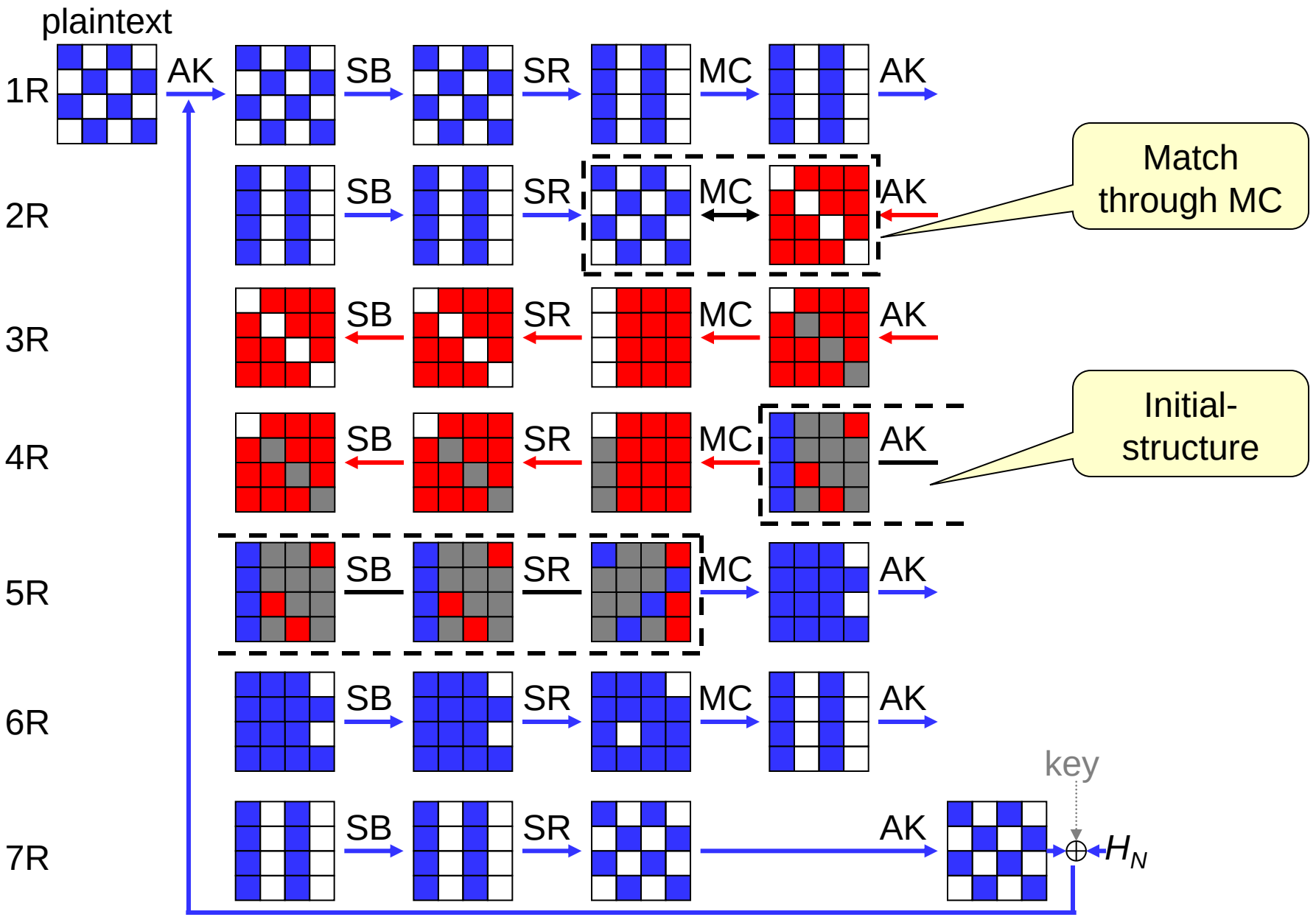
NTT

7-round attack

7R AES



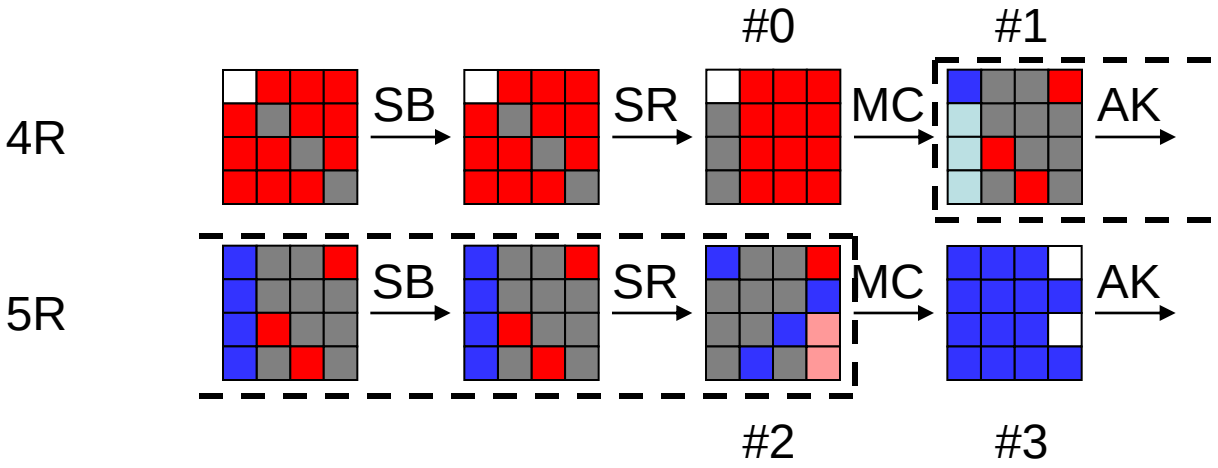
7R AES


plaintext
1R
2R
3R
4R
5R
6R
7R
AK
SB
SR
MC
AK
Match through MC
Initial-structure
key
H_N

Initial-structure

Byte position

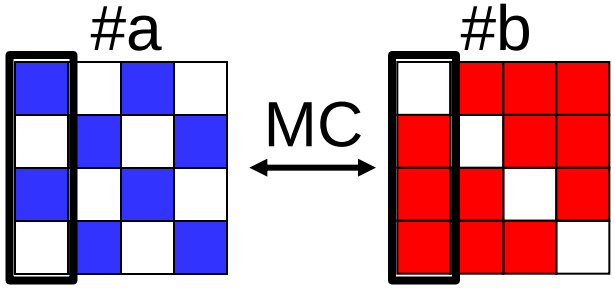
0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15



- #1 is the start point for the forward chunk.
- For all 2^8 values of 0^{th} byte of #1, compute 1^{st} to 3^{rd} bytes of #1 so that 1^{st} to 3^{rd} bytes of #0 becomes a pre-specified constant.
- Then, backward chunk from #0 (Red) can start 15 known bytes at #0.

Match through MC (1/2)

2^8 candidates



2^8 candidates

Focus on the left most column

$$\#a[0] = ({}_xe \cdot \#b[0]) \oplus ({}_xb \cdot \#b[1]) \oplus ({}_xd \cdot \#b[2]) \oplus ({}_x9 \cdot \#b[3])$$
$$\#a[2] = ({}_xd \cdot \#b[0]) \oplus ({}_x9 \cdot \#b[1]) \oplus ({}_xe \cdot \#b[2]) \oplus ({}_xb \cdot \#b[3])$$

$$\begin{cases} \#a[0] \oplus C_0 = {}_xe \cdot \#b[0] \\ \#a[2] \oplus C_1 = {}_xd \cdot \#b[0] \end{cases}$$

- Without knowing #b[0], we can match by checking the ratio of two values.

Match through MC (2/2)

$$\begin{cases} \#a[0] \oplus C_0 = {}_xe \cdot \#b[0] \\ \#a[2] \oplus C_1 = {}_xd \cdot \#b[0] \end{cases}$$

- Idea from indirect partial-matching for the efficient match.

$$\#a[0] \cdot {}_xd \oplus C_0 \cdot {}_xd = \#a[2] \cdot {}_xe \oplus C_1 \cdot {}_xe$$

$$\#a[0] \cdot {}_xd \oplus \#a[2] \cdot {}_xe = C_0 \cdot {}_xd \oplus C_1 \cdot {}_xe$$

Match with this equation

In the computation of each chunk, we compute the above values used in the match.

Summary of 7-Round Attack

- Both chunks have 8-bit freedom degrees.
- Efficient match with match through MC.

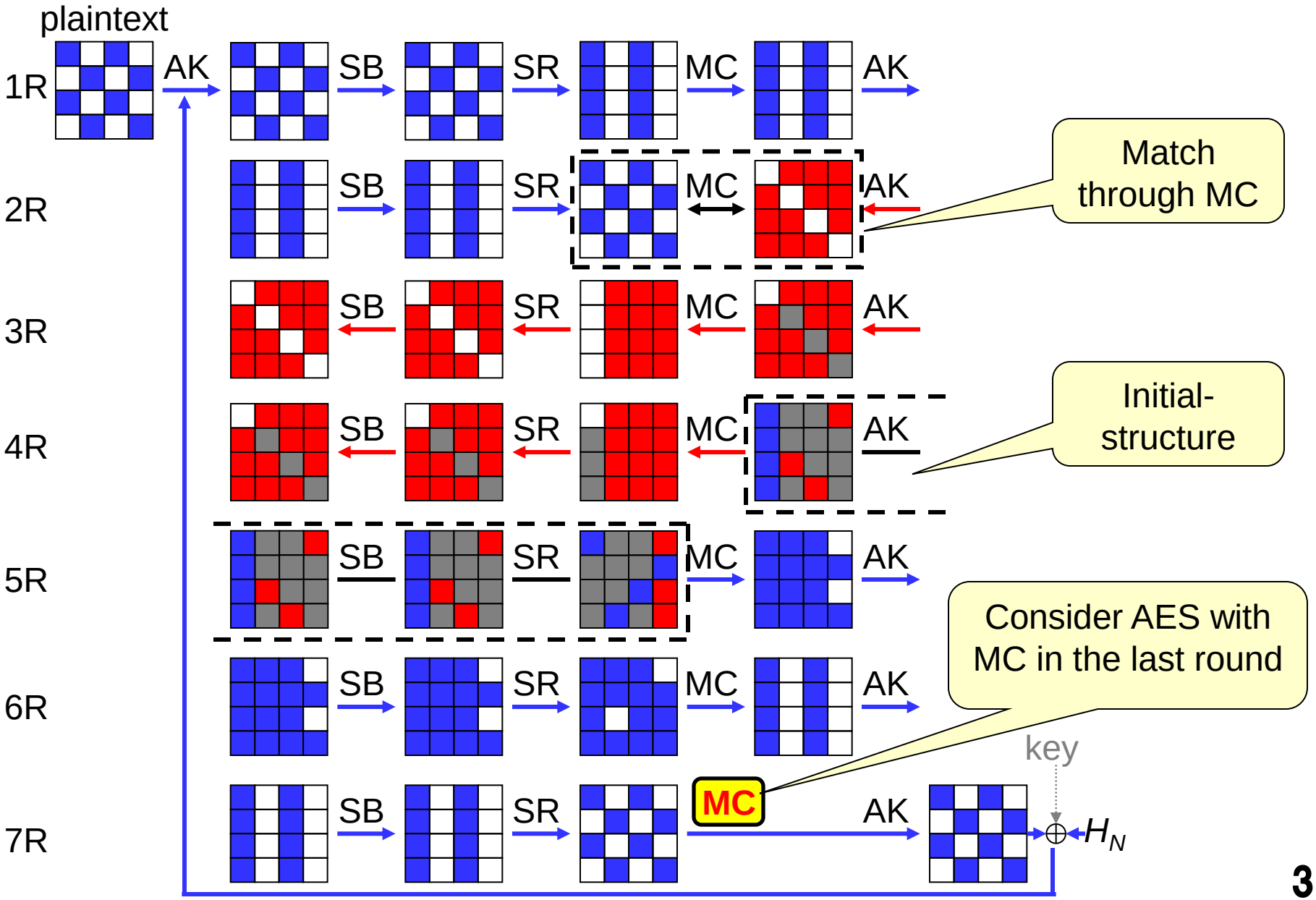
- Pseudo-preimages are found faster than brute force attack by a factor of 2^8 ($=2^{120}$).

NTT

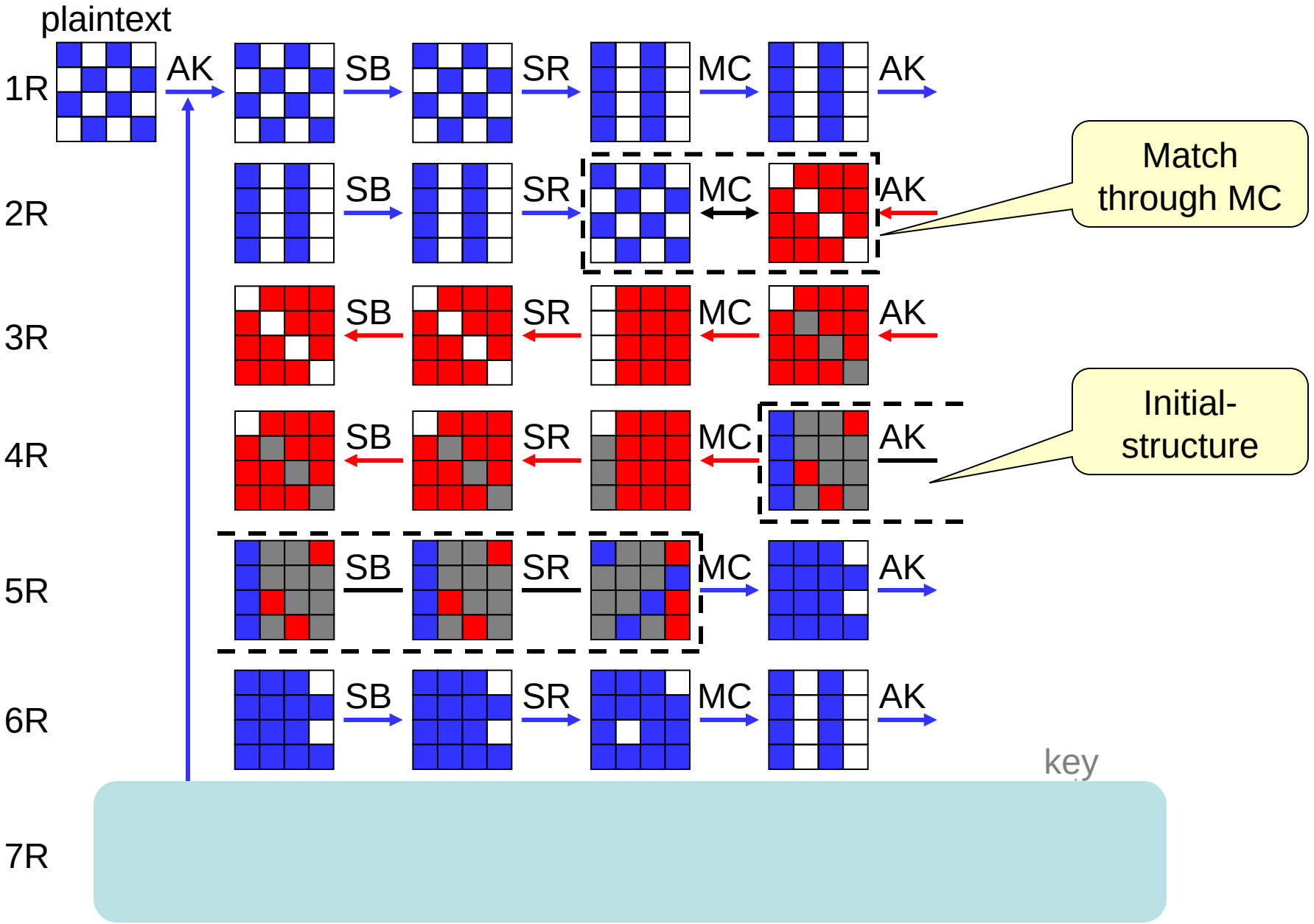
Outline

- Motivation
- Problems of current techniques
- Our attacks
- Application to Whirlpool

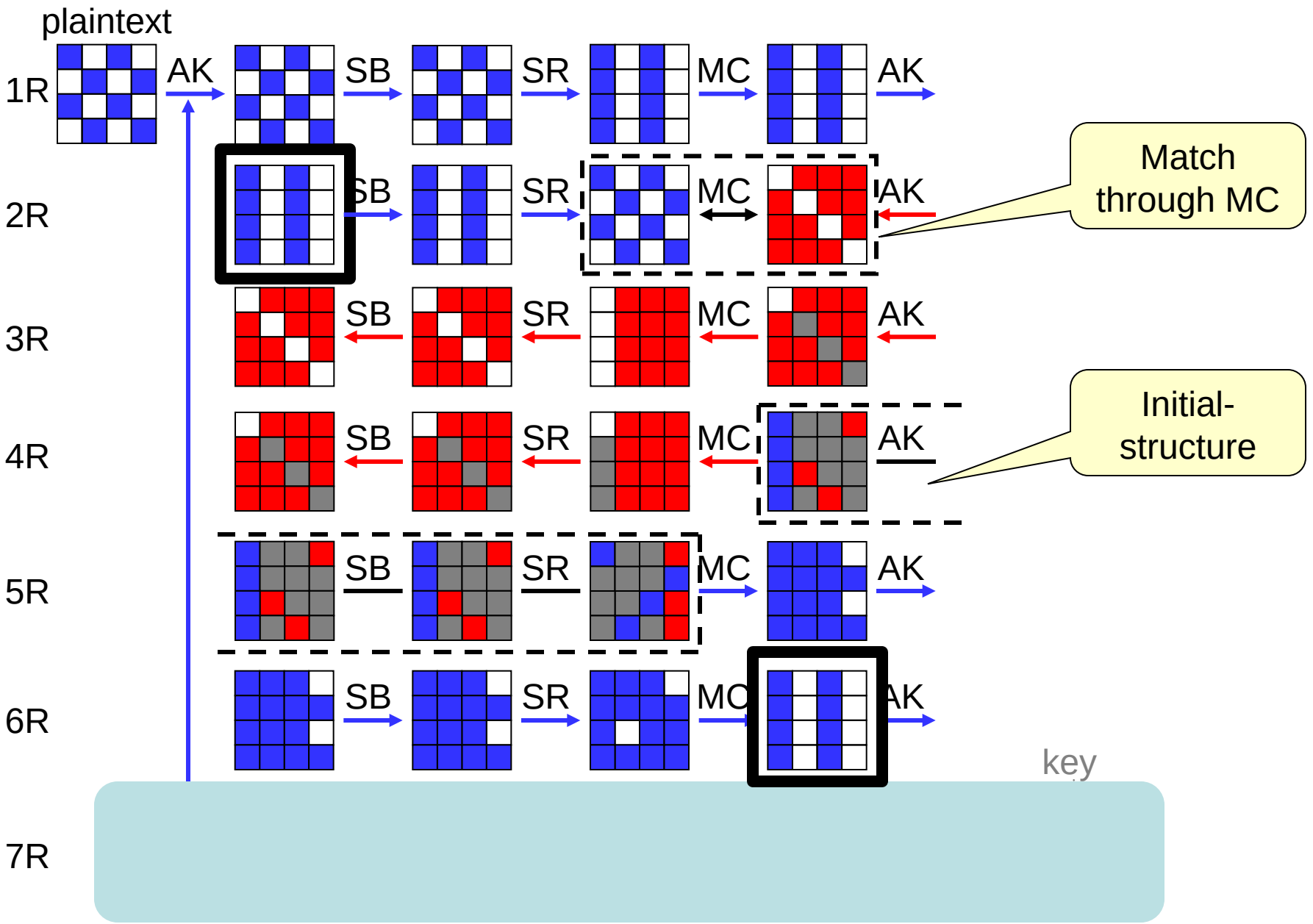
AES with MC in the last



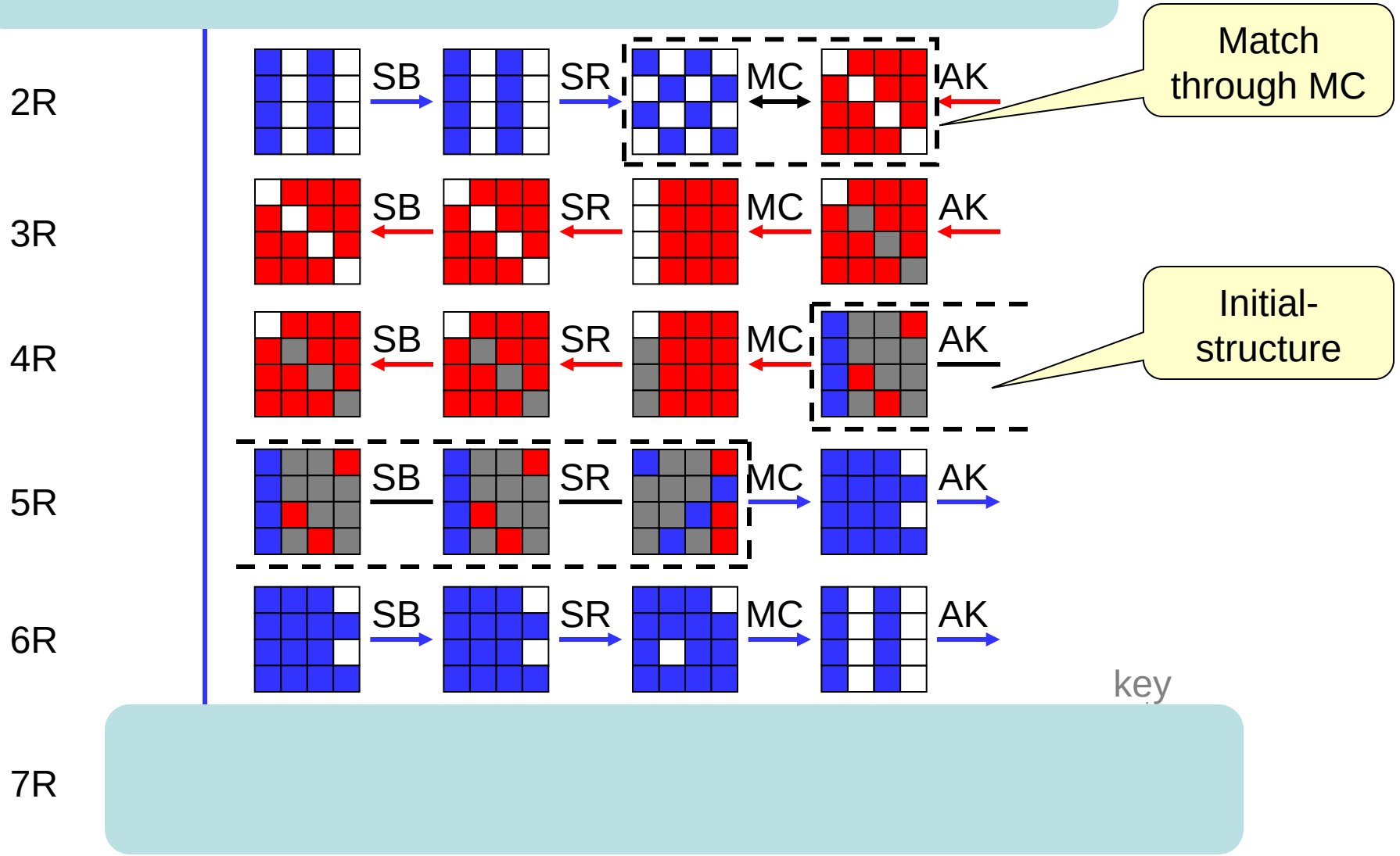
AES with MC in the last



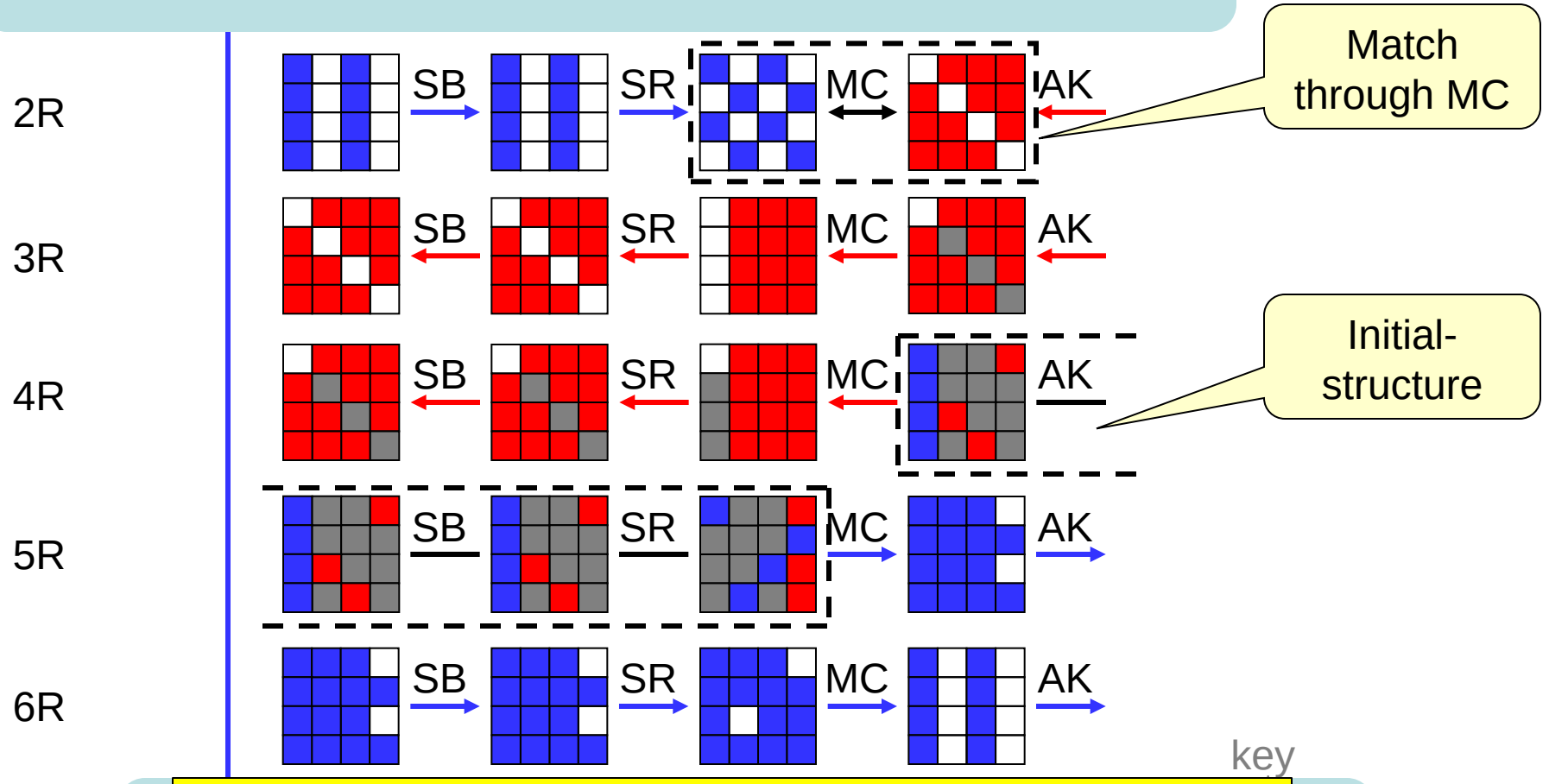
AES with MC in the last



AES with MC in the last



AES with MC in the last



The attack works up to 5 rounds.
Whirlpool is attacked up to 5 rounds.

NTT

Summary

- Preimage attacks on AES hashing modes
  - First results on preimages of AES based structure.
  - First results on the application of MitM preimage attacks on AES.
  - Attack reaches 7 rounds of AES-hash and 5 rounds of Whirlpool.
- Used a slow diffusion when we start the analysis from the second last round.

NTT

Thanks for your attention !!

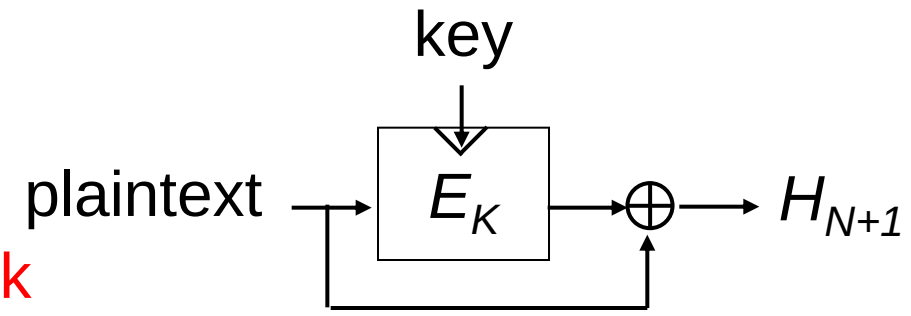
Q & A

Conversion to Preimages or Second Preimages

- The key is fixed and the plaintext is randomly determined during the attack.
- Assume the Merkle-Damgård structure as a domain extension.

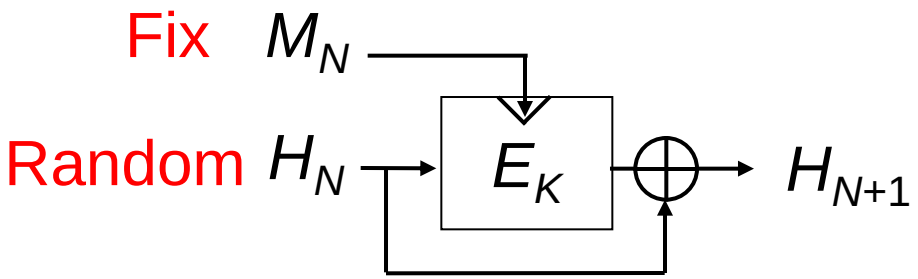
Fixed to the value of attacker's choice

randomly determined during the attack



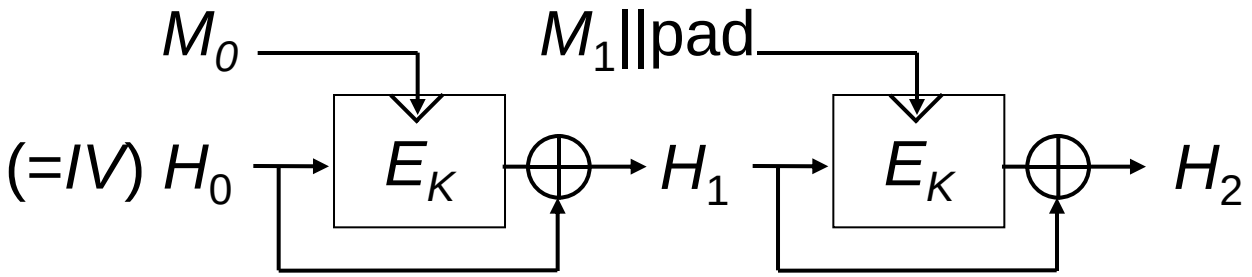
Conversion in DM-Mode

Davies-Mayer mode



M_N can be chosen so that padding is satisfied.

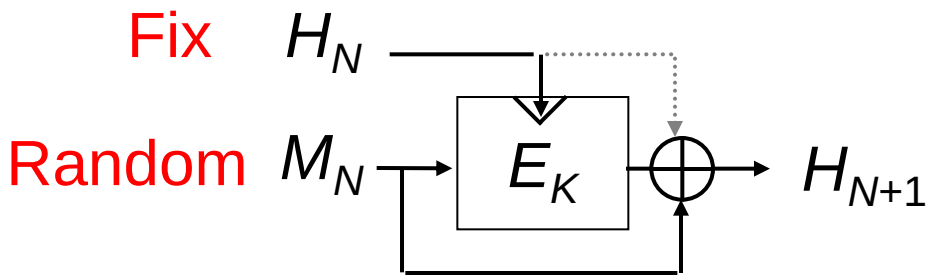
H_N cannot be fixed to IV. Use a generic conversion.



Preimage attack in 2 blocks. Compleixty: 2^{125}.

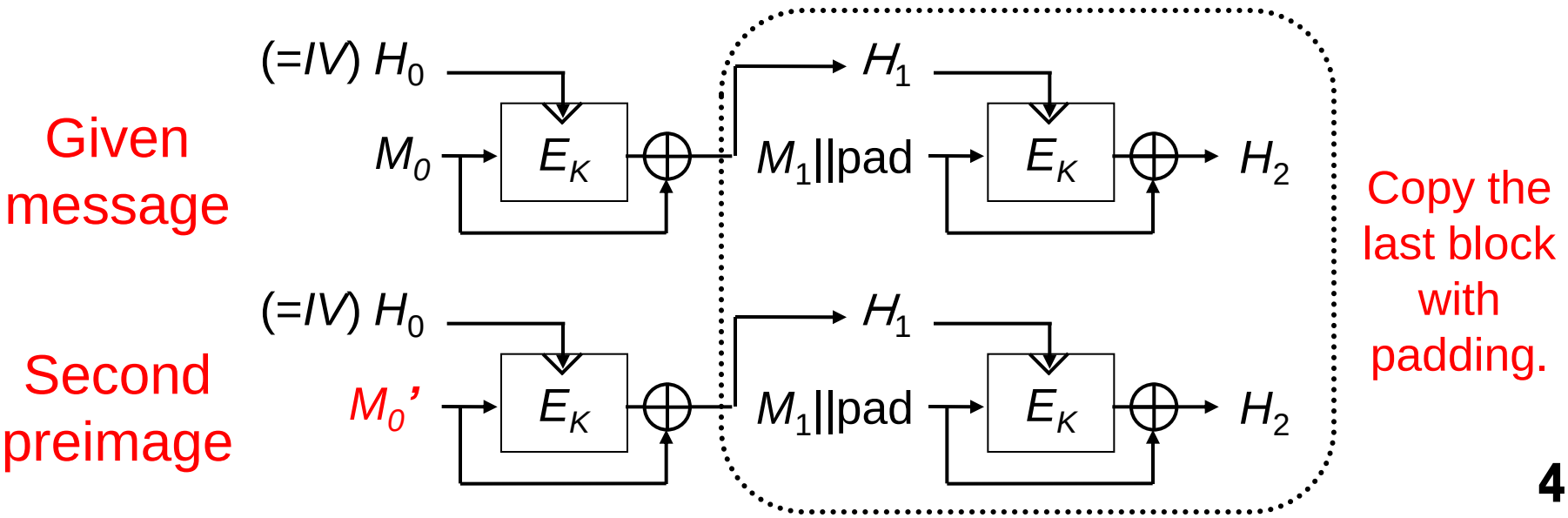
Conversion in MMO/MP modes

MMO/MP modes



H_N can be fixed to IV.

M_N cannot satisfy padding. ➡ Second preimage attack

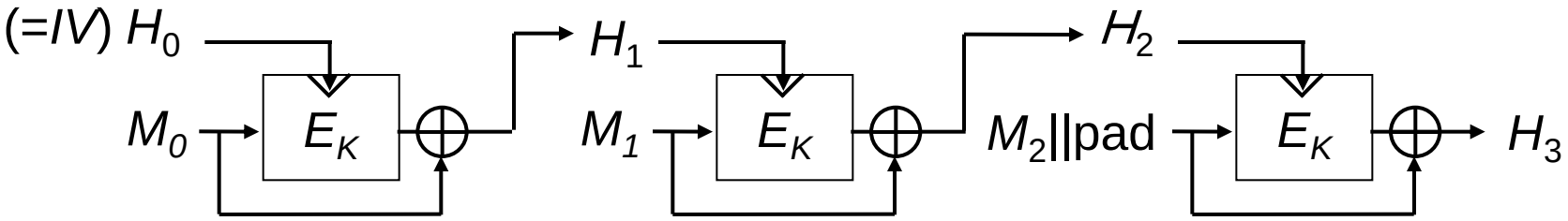


Conversion in MMO/MP modes

Not enough freedom degrees because is *H* fixed.

Increases freedom degrees to make a 3-block attack.

Given message



Prepare a list of H_1'.

Second preimages