Equivalent Key Recovery Attacks against HMAC and NMAC with Whirlpool Reduced to 7 Rounds

Jian Guo[1], **Yu Sasaki**[2], Lei Wang[1],
Meiqin Wang[3] and Long Wen[3]

1: Nanyang Technological University, Singapore
2: NTT Secure Platform Laboratories, Japan
3: Shandong University, China

FSE 2014 (05/March/2014)

Initially discussed at ASK 2013 at Weihai

Research Summary

- Improved key recovery attack on HMAC-Whirlpool
- Convert MitM attacks on AES based ciphers into the known plaintext model.

Key type	#Rounds	Complexity			Reference
		Time	Memory	Data	
Original Key	5	2^{402}	2^{384}	2^{384}	[14]
	6	2^{496}	2^{448}	2^{384}	[14]
Equivalent Keys	5	2^{448}	2^{377}	2^{321}	[14]
	6	2^{451}	2^{448}	2^{384}	[14]
	7	$\mathbf{2^{490.3}}$	$\mathbf{2^{481}}$	$\mathbf{2^{481.7}}$	**Ours**

$2^{482.3}$ for camera-ready version

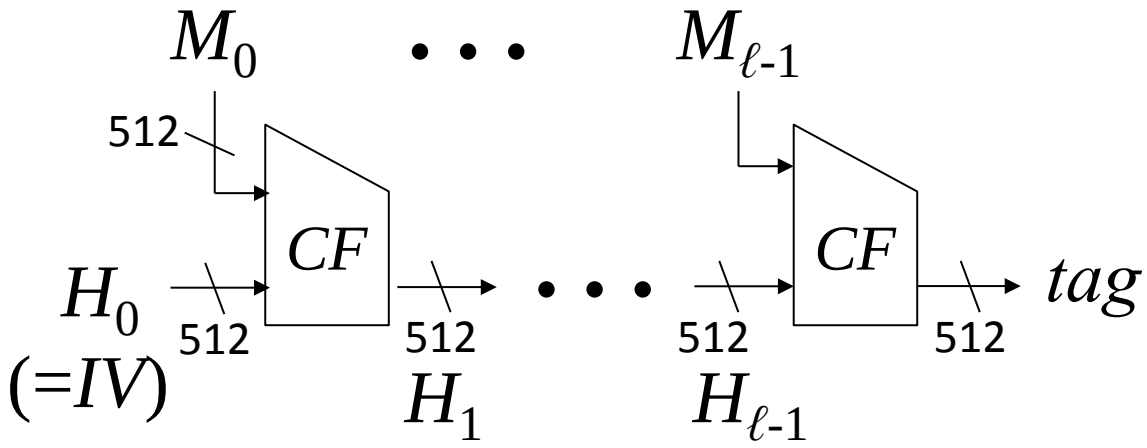
NTT

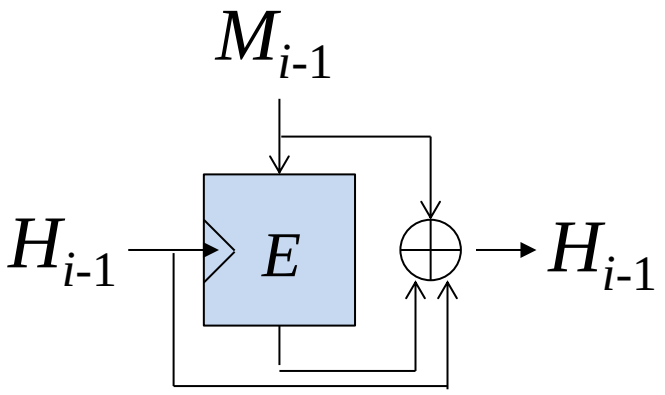
Whirlpool

- AES based 512-bit hash function proposed by Barreto and Rijmen in 2000
- Standardised by ISO
- Recommended by NESSIE
- Implemented in many cryptographic libraries
- Its usage in HMAC is also implemented.

More Structure on Whirlpool

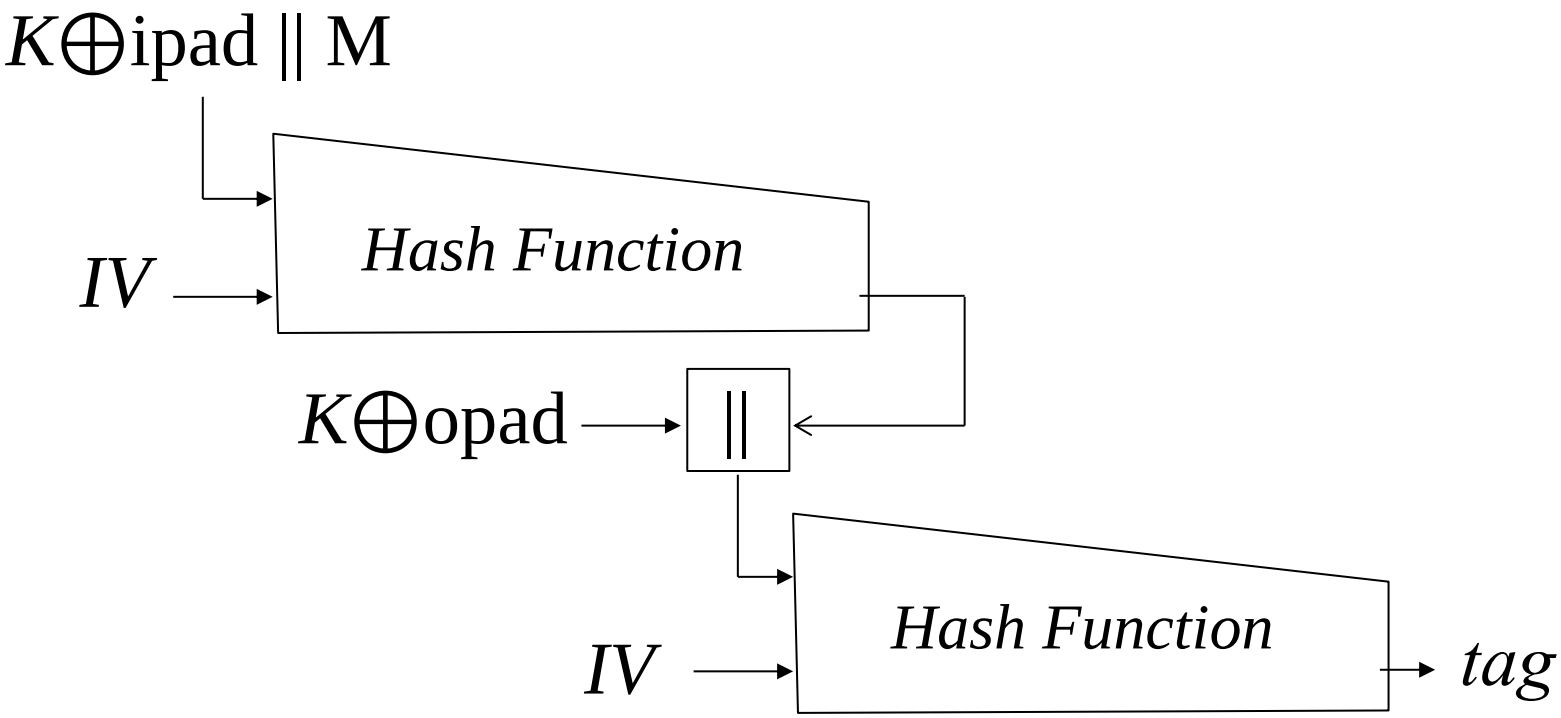
- Narrow-pipe Merkle-Damgård iteration
- Compression function is built by Miyaguchi-Preneel mode with an AES based block-cipher.





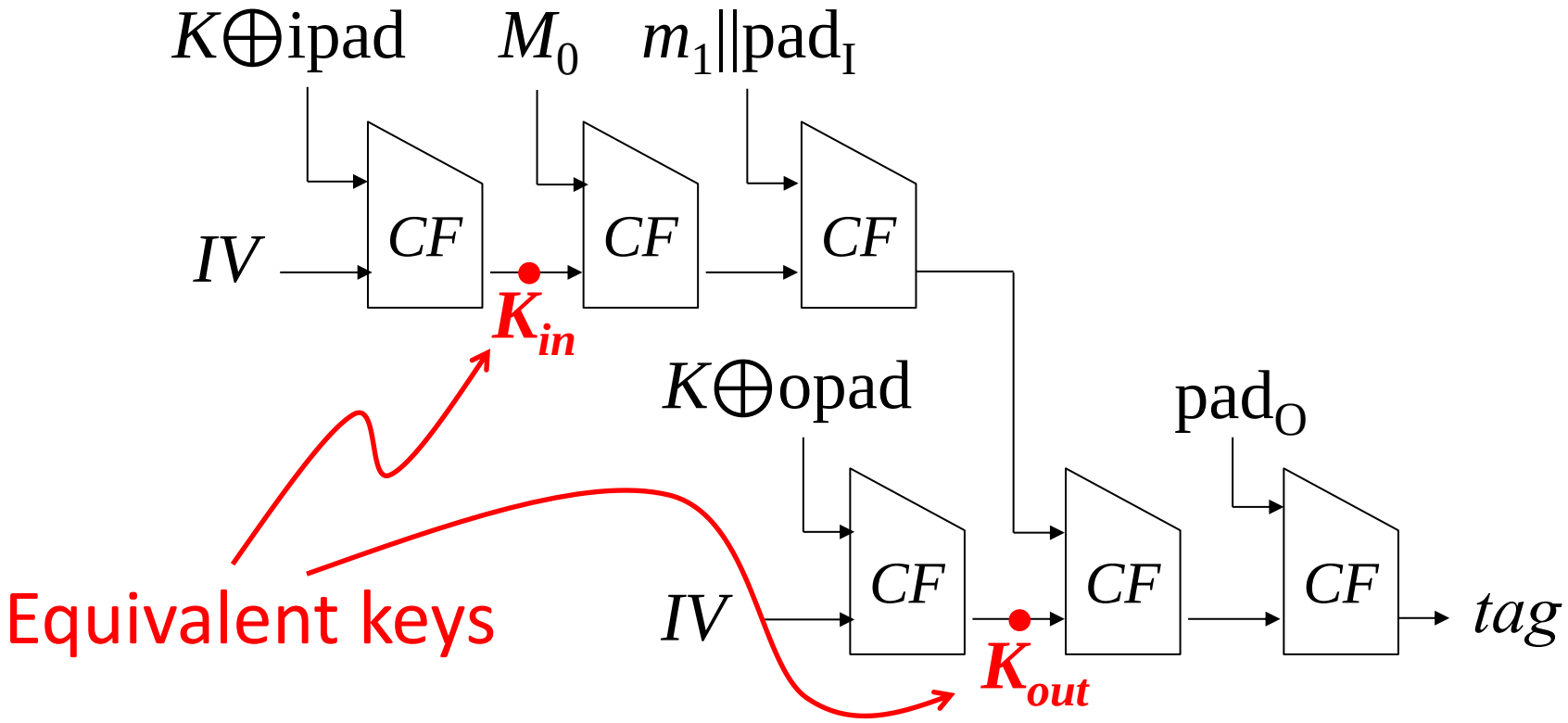
HMAC

- Proposed by Bellare et al. in 1996 with a proof of being PRF up to the birthday order queries.
- Generating a MAC by two hash function calls



HMAC in CF Level

- Proposed by Bellare et al. in 1996 with a proof of being PRF up to the birthday order queries.
- Generating a MAC by two hash function calls



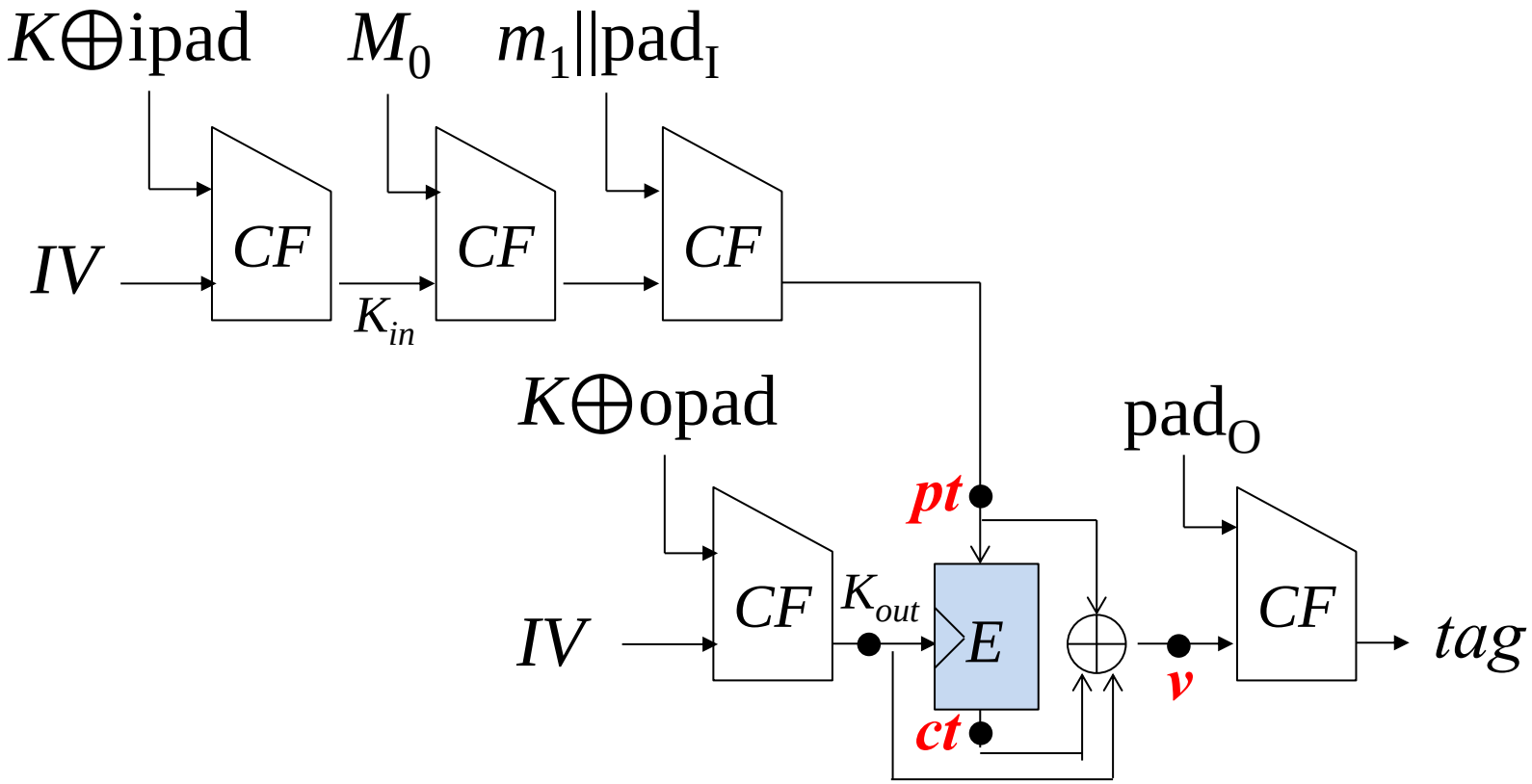
NTT

Initial Thoughts

- Previous key recovery attack on HMAC-Whirlpool is up to 6 rounds.
- At Eurocrypt 2013, Derbez et al. presented 7-round key recovery attack on AES with a MitM attack in the chosen-plaintext model.
- Can we apply the MitM attack to 7-round HMAC-Whirlpool?
- The application is not easy!!

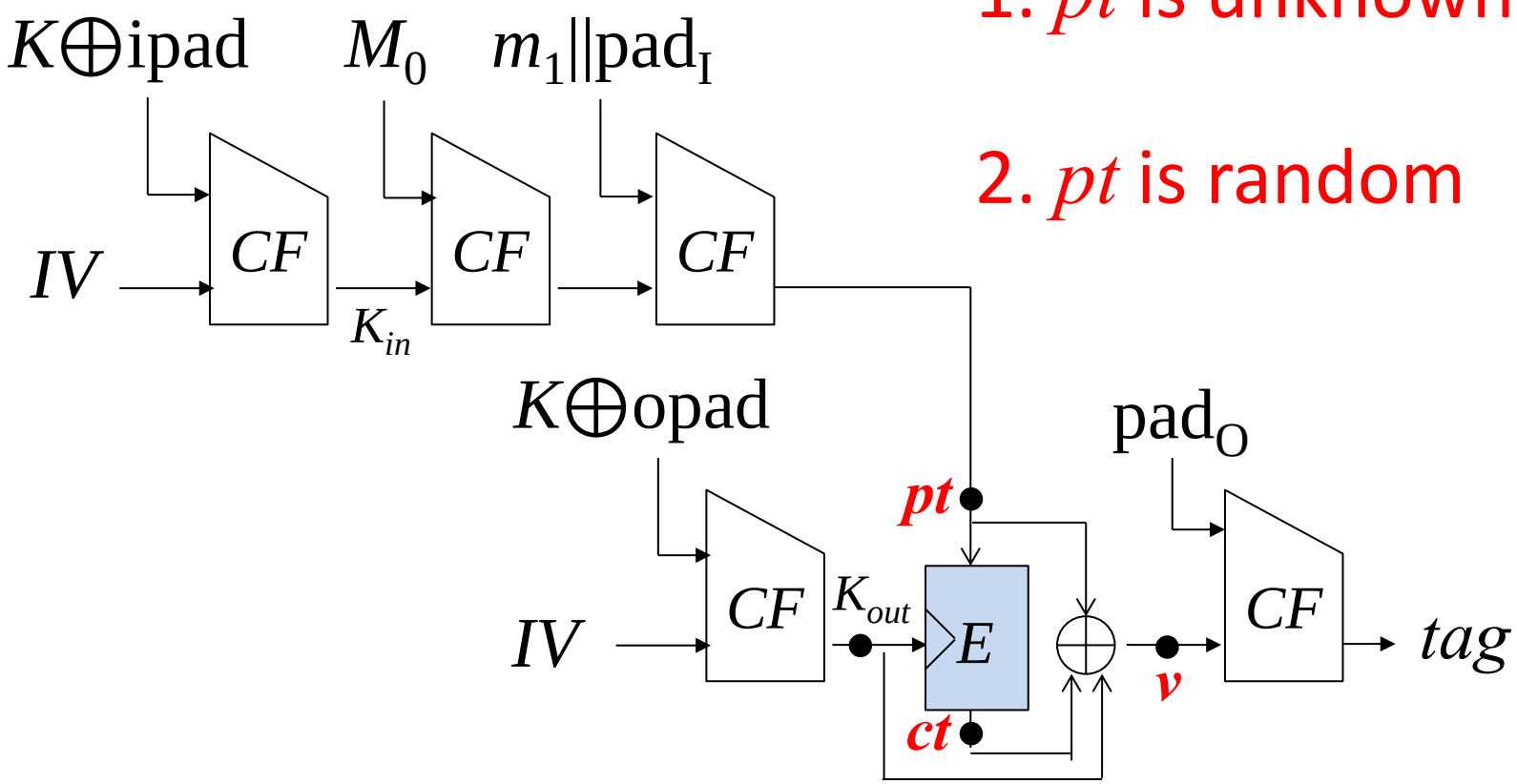
Overview

- Collect many pairs of (pt, ct) and run the MitM attack.
- K_{out} is used as a key input of the AES-based cipher. It should be recovered by the MitM attack.



Difficulties of MitM Attack

- In HMAC, the attacker only can observe *tag* value.



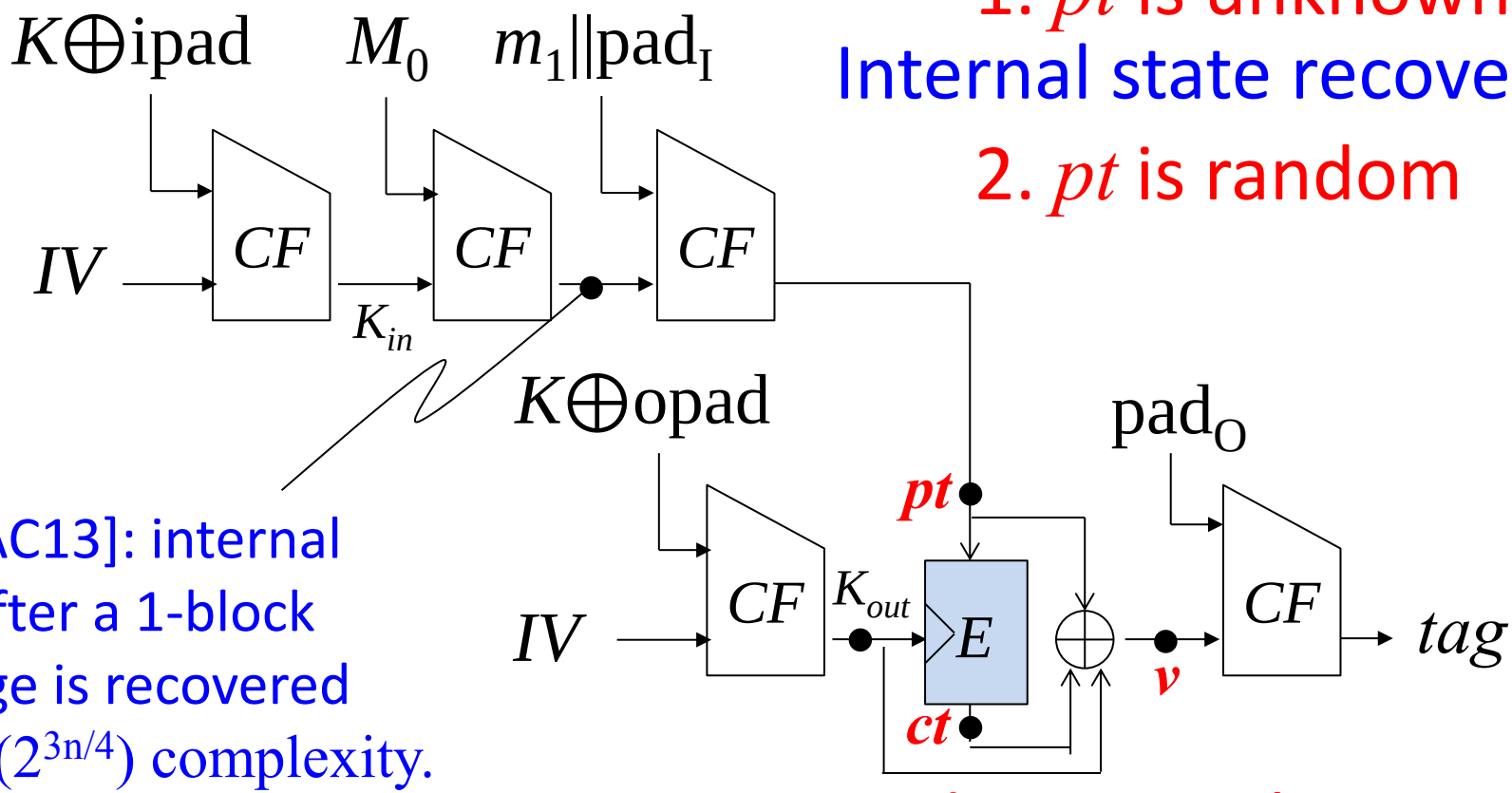
1. *pt* is unknown

2. *pt* is random

3. *v* and *ct* are unknown

Our Strategy for Difficulty 1

- In HMAC, the attacker only can observe *tag* value.



1. *pt* is unknown

Internal state recovery

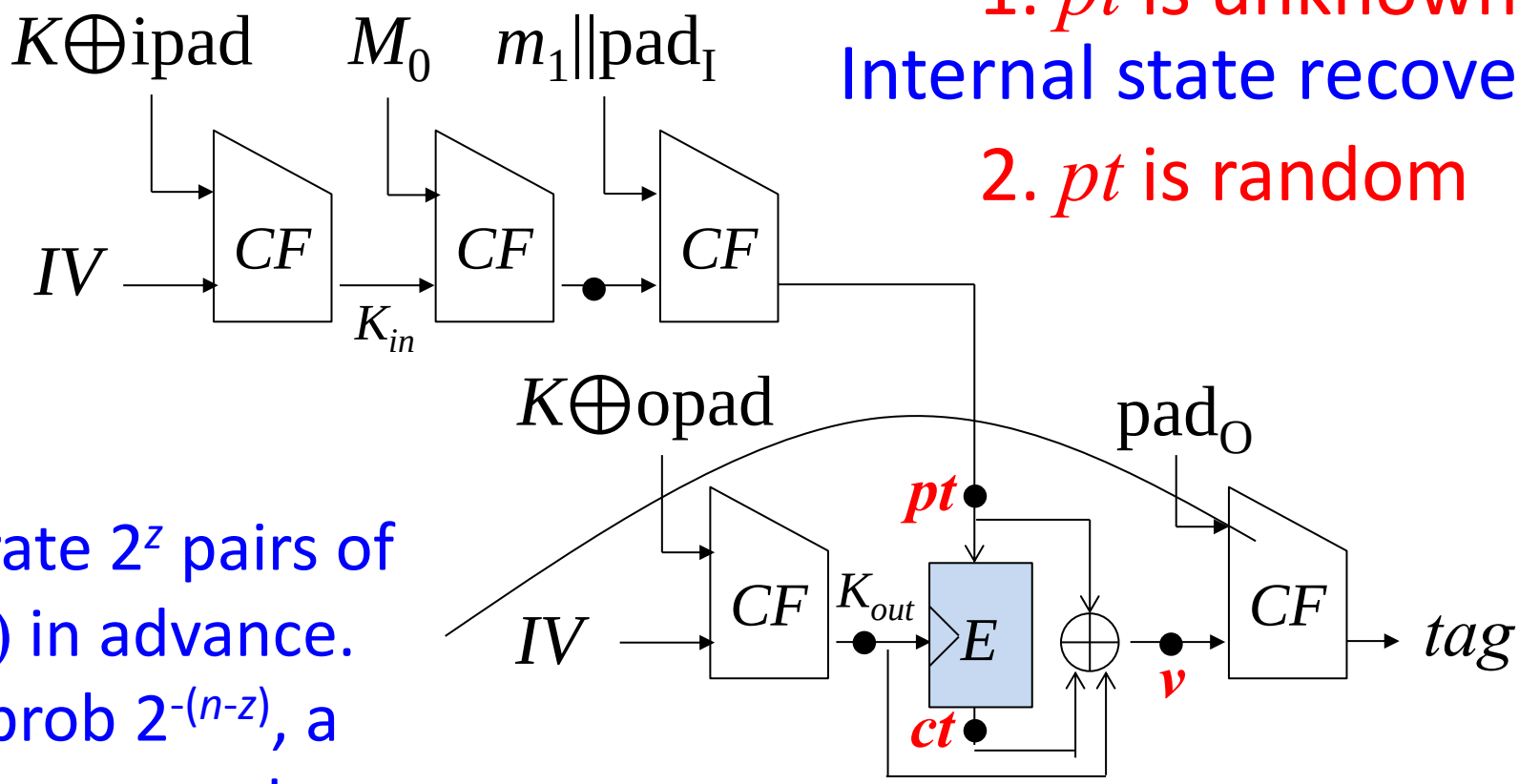
2. *pt* is random

[LPW-AC13]: internal state after a 1-block message is recovered with $O(2^{3n/4})$ complexity.

3. *v* and *ct* are unknown

Our Strategy for Difficulty 3

- In HMAC, the attacker only can observe *tag* value.



1. *pt* is unknown
Internal state recovery

2. *pt* is random

Generate 2^z pairs of (v,tag) in advance.
With prob $2^{-(n-z)}$, a *tag* is converted to *v*.

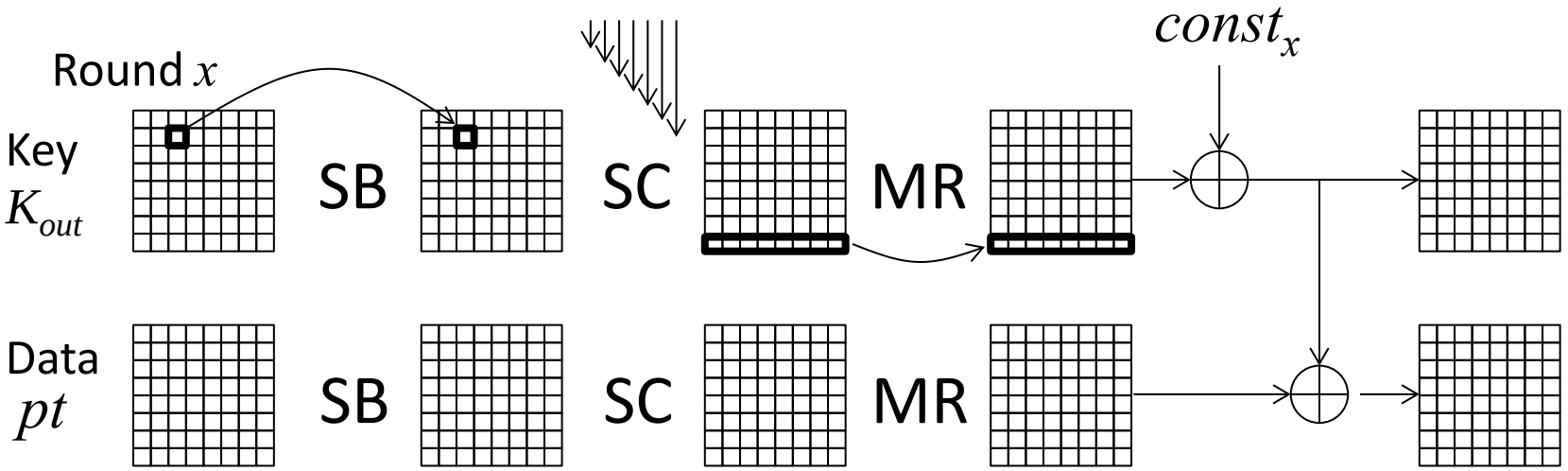
3. *v* and *ct* are unknown
Precompute look-up table

NTT

MitM Attacks on AES Based Ciphers in Known Plaintext Model

Whirlpool Internal Block-cipher

- 8×8-byte state
- 10 rounds, with the last MixRows operation
- Similar operations between key and data



Notations: δ-set and n-δ-set

For a byte-oriented cipher, a δ-set is a set of 256 texts such that a byte takes all possible values among 256 texts (***A**ctive*) and the other bytes take a fixed value (***C**onstant*) among 256 texts. If n bytes are active, we call it n-δ-set.

δ-set

A	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*

12-δ-set used in our attack

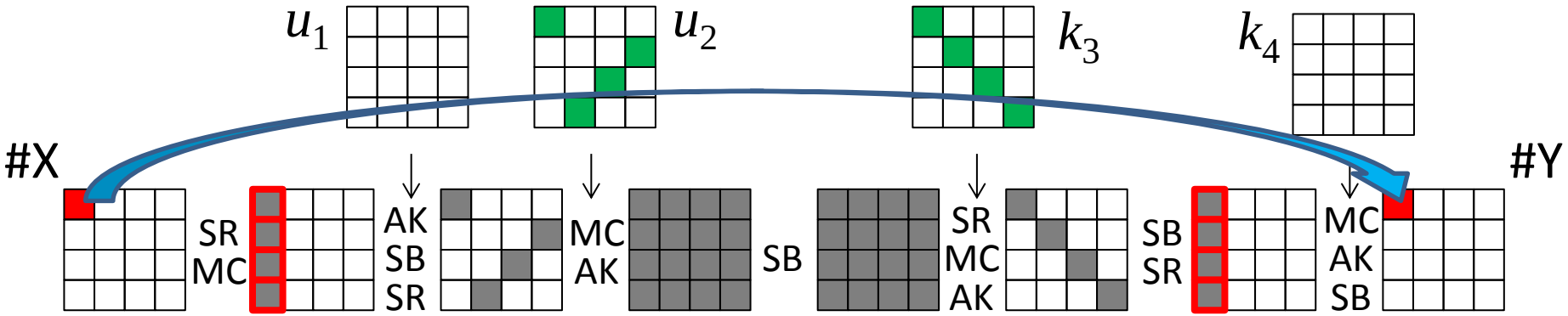
A	***A***	***A***	*C*	*C*	*C*	*C*	*C*
A	***A***	*C*	*C*	*C*	*C*	*C*	***A***
A	*C*	*C*	*C*	*C*	*C*	***A***	***A***
C	*C*	*C*	*C*	*C*	***A***	***A***	***A***
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*
C	*C*	*C*	*C*	*C*	*C*	*C*	*C*

Previous MitM Attack on AES (1/2)

- 7R characteristic: 4 -> 1 -> 4 -> 16 -> 4 -> 1 -> 4 -> 16

E_{pre} E_{mid} E_{post}

- 4-round middle distinguisher



– Consider a function f which maps #X[0] to #Y[0]. The number of all possible such functions is $2^{8*256}=2^{2048}$

– For a pair of texts satisfying the characteristic, construct a δ-set by modifying #X[0], $(\delta_0,\delta_1,\ldots,\delta_{255})$. Then, $\{f(\delta_0),f(\delta_1),\ldots,f(\delta_{255})\}$ can take only 2^{80} possibilities.

Previous MitM Attack on AES (2/2)

- 7-round characteristic

2^{80} possibilities

Offline: precompute 2^{80} possibilities of distinguishers.

Online: collect pairs of plaintext and ciphertext satisfying the input and output differential forms.

- For each pair, guess sk_{pre} and change plaintext so that a δ-set is constructed at #X[0].
- For each modified plaintext, obtain the ciphertext.
- Guess sk_{post} and match precomputed distinguishers

NTT

Is It Applicable to HMAC-Whirlpool?

The answer is not obvious.

- Chosen-plaintext v.s. Known-plaintext
  - Cannot efficiently collect plaintext pairs
  - After constructing δ-set at #X[0], the corresponding ciphertext is obtained only probabilistically.

    (multi-set technique cannot be used)
- 4*4 state size v.s. 8*8 state size
  - Larger state of Whirlpool is easier to analyze
  - (2^{-468} for multiset technique is no longer enough)
- Whirlpool key schedule is easier to analyze

NTT

Our Strategy

- Chosen-plaintext v.s. Known-plaintext
  - Cannot efficiently collect plaintext pairs

  Simply increasing the data amount.

  - After constructing δ-set at #X, the corresponding ciphertext is obtained only probabilistically.

    (multi-set technique cannot be used)

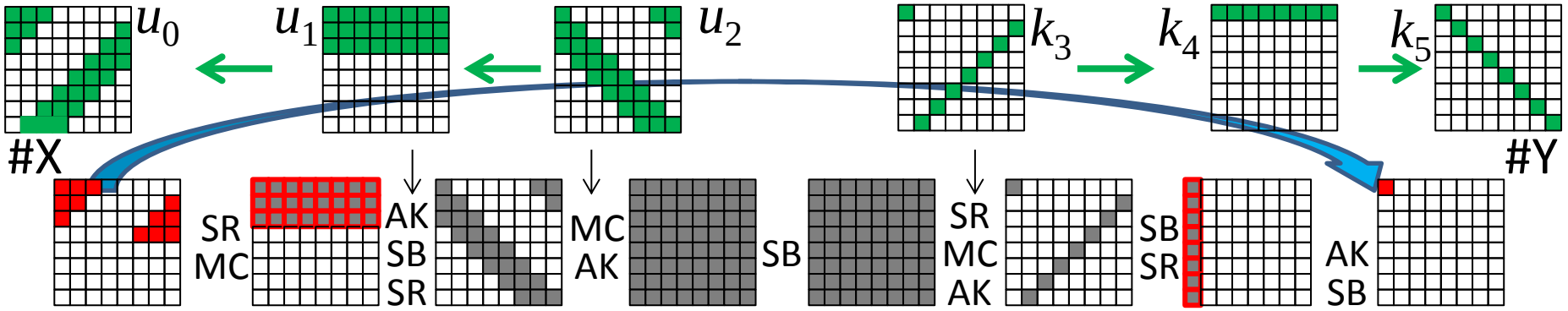
  Use n-δ-set instead of δ-set →
  more elements are examined, and
  enough elements will remain

MitM Attack on HMAC-Whirlpool (1/4)

- 7R characteristic: 32 -> 12 -> 24 -> 64 -> 8 -> 1 -> 8 -> 64

E_{pre} E_{mid} E_{post}

- 4-round middle distinguisher



  - Consider a function f which maps 12 bytes of #X to #Y[0]. The number of all such functions is so huge.
  - For a pair of texts satisfying the characteristic, construct a 12-δ-set by modifying #X, $(\delta_0,\delta_1,\ldots,\delta_{2\text{^}96-1})$. Then, $\{f(\delta_0),f(\delta_1),\ldots,f(\delta_{2\text{^}96-1})\}$ takes 2^{360} possibilities.

MitM Attack on HMAC-Whirlpool (2/4)

- 7-round characteristic

2^{360} possibilities

Offline: precompute 2^{360} possibilities of distinguishers.

Online: collect pairs of plaintext and ciphertext satisfying the input and output differential forms.

- For each pair, guess sk_{pre} and change plaintext so that a 12-δ-set is constructed at #X.

!!

- For each modified plaintext, obtain the ciphertext.

- Guess sk_{post} and match precomputed distinguishers

MitM Attack on HMAC-Whirlpool (3/4)

1. Due to the known-plaintext model, only a part of 12-δ-set can be obtained.

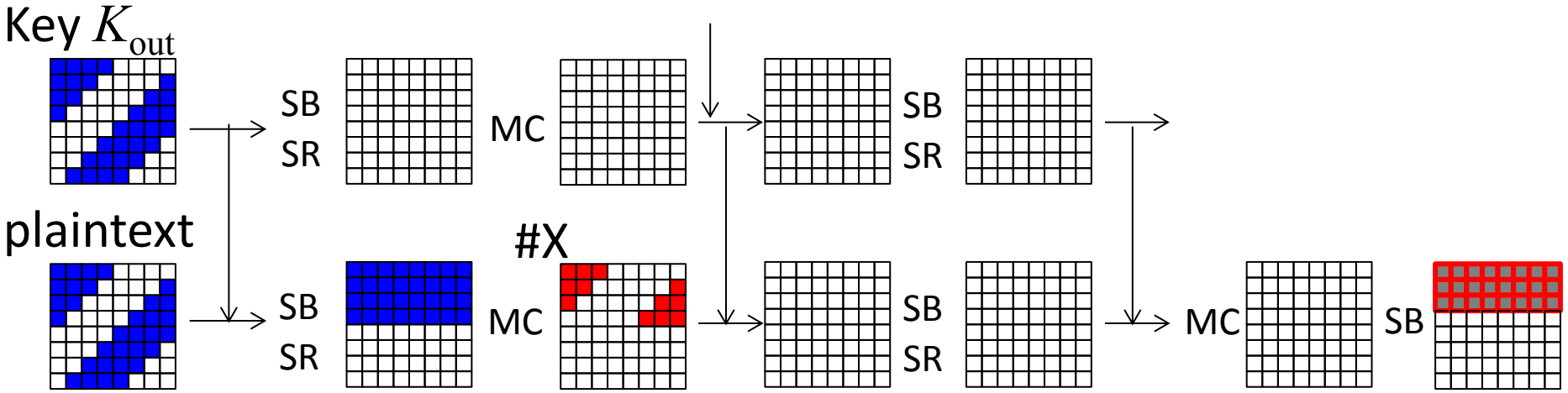
2. Due to the conversion from tag to ct, ct is obtained only probabilistically.

➡ can resolve by using more data

3. Cannot know which element of 12-δ-set is obtained. Cannot sort the precomputation table. (match cost ≠ 1.)

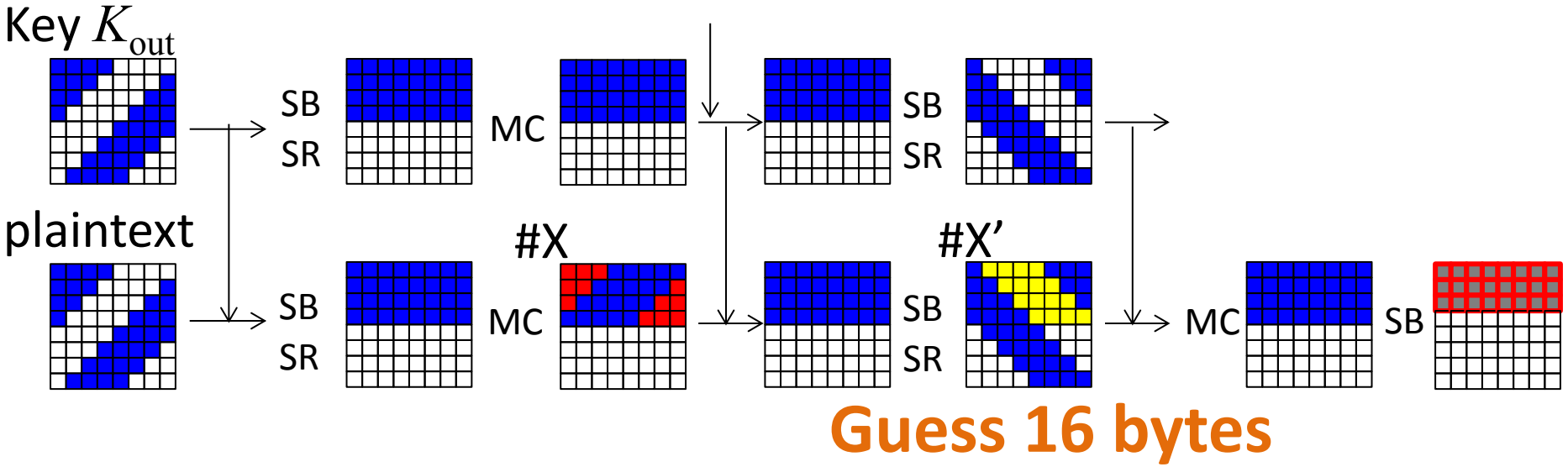
1. - For each pair, guess sk_{pre} and change plaintext so that a 12-δ-set is constructed at #X.
2. - For each modified plaintext, obtain the ciphertext.
3. - Guess sk_{post} and match precomputed distinguishers

MitM Attack on HMAC-Whirlpool (4/4)



- Previous attack only recovers up to #X.

MitM Attack on HMAC-Whirlpool (4/4)

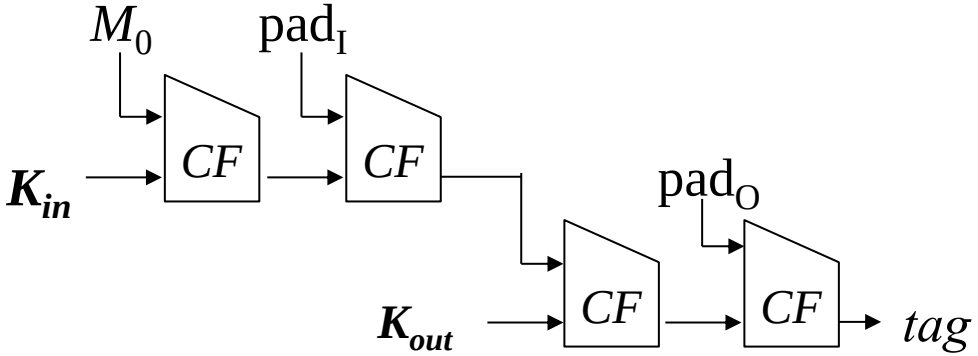


- Previous attack only recovers up to #X.
- In Whirlpool, we know more bytes. By guessing more bytes at #X', we can recover all bytes which are index of 2^{360} distinguisher.
- The match is done for the sorted data.

Remarks on Attacks

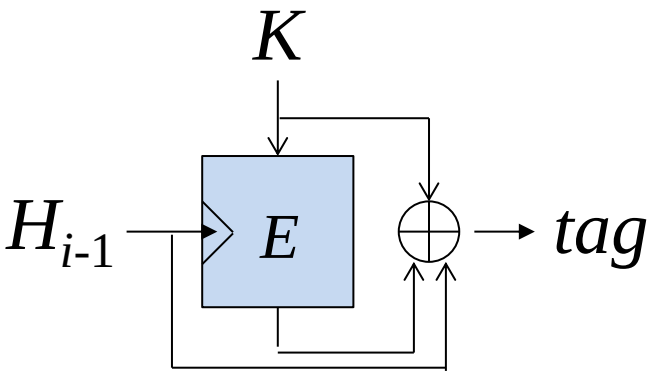
- The best diff characteristic and the number of n-δ-set were searched by programming.
- An optimization technique for making conversion table from tag to v.
- (Time, Mem, Data) = ($2^{490.3}$, 2^{481}, $2^{481.3}$)

  ➡ $2^{482.3}$ for camera-ready
- K_{in} recovery is easier because it is CPA, not KPA.



Concluding Remarks

- 7-round key recovery attack on HMAC-Whirlpool
- Based on MitM attack on AES, but many different problems and many optimizations for HMAC and AES-based compression functions
- Application to Sandwich-MAC still opens.
  - needs unknown plaintext recovery with different keys



Thank you !!