Cryptanalysis of Haraka

Jérémy Jean

Agence Nationale de la Sécurité des Systèmes d'Information

Crypto Laboratory

FSE 2017 @ Tokyo, Japan

March 6, 2017

Jeremy.Jean@ssi.gouv.fr

Introduction

Let n be a positive integer (typically, $n = 128$, $n = 160$ or $n = 256$)

General Hash Function

- ''Securely'' hashes any string to a fixed-width n-bit string
- $h : \{0,1\}^* \longrightarrow \{0,1\}^n$
- Required security levels:
  - (Second) preimage resistance: n bits
  - Collision resistance: $n/2$ bits
- Examples: SHA-2, SHA-3, etc.

Hash Function for Hash-Based Signature Schemes

- Why? Used in a few schemes for PQ crypto:

  e.g., Lamport [Lam79], XMSS [BDH11], SPHINCS [BHH+15]
- One **pair** of short-input hash functions:

$$h_n : \{0,1\}^n \longrightarrow \{0,1\}^n \text{ and } h_{2n} : \{0,1\}^{2n} \longrightarrow \{0,1\}^n$$

- Only required security: n-bit (second) preimage resistance
- Example: Haraka ($n = 256$)
- **No collision resistance**: non-trivial to adapt usual design strategies to drop this security requirement

Specifications of Haraka: High-Level Overview

Haraka: Two Functions

$$\text{Haraka-256/256} : \{0,1\}^{256} \longrightarrow \{0,1\}^{256}$$

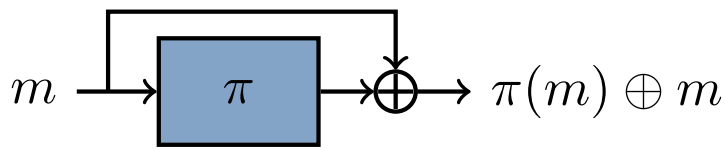
$$\text{and: } \quad \text{Haraka-512/256} : \{0,1\}^{512} \longrightarrow \{0,1\}^{256}$$

Haraka-256/256

- Internal state: 256 bits
- Davies-Meyer mode
- Inner permutation: π_{256}
- Output size: 256 bits

Haraka-512/256

- Internal state: 512 bits
- Davies-Meyer mode
- Inner permutation: π_{512}
- Output size: 256 bits
- Final truncation



Claimed Security

- 256-bit preimage security [Broken]
- Stronger Haraka variant: 128-bit collision security [Broken]

Haraka-256/256

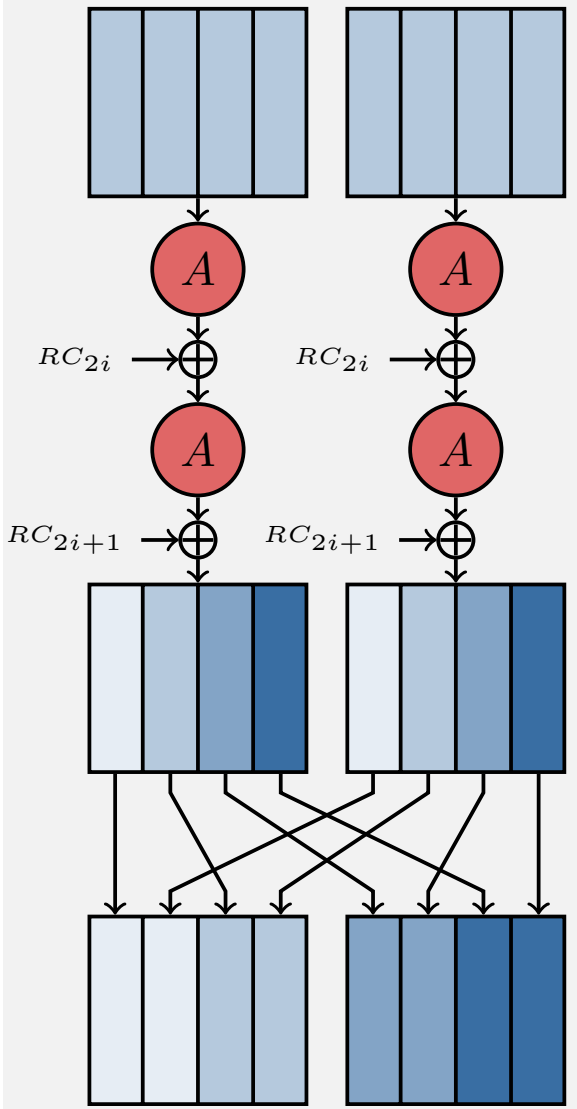
Inner Permutation π_{256}

- Internal state: 2 AES states
- Repeat 5 steps ($i = 0, \ldots, 4$):
  - Apply 1R AES on each state w/ key RC_{2i}
  - Apply 1R AES on each state w/ key RC_{2i+1}
  - Permute the AES columns (**mix**)
- Final Davies-Meyer feed-forward

Claimed Security

- **Preimage resistance:**
  - #steps: 5
  - Security level: 256 bits
- **Collision resistance:**
  - #steps: 6 (stronger)
  - Security level: 128 bits

One step of π_{256}



Haraka-512/256

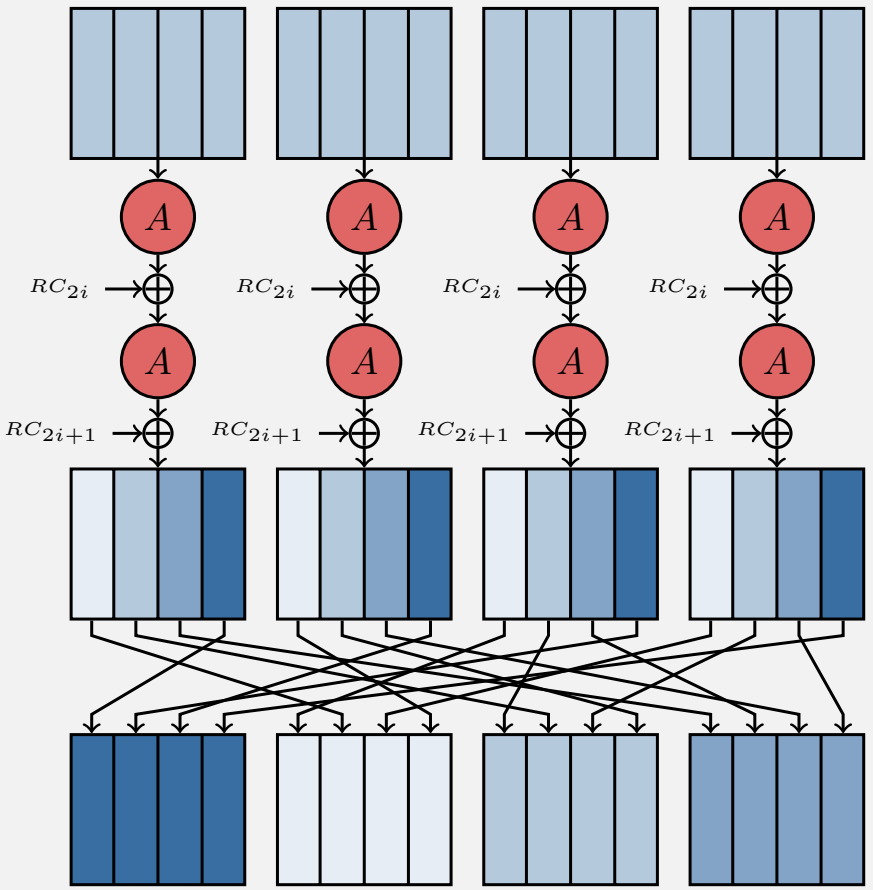
Inner Permutation π_{512}

- Same principle as π_{256}
- Final truncation to produce 256 bits

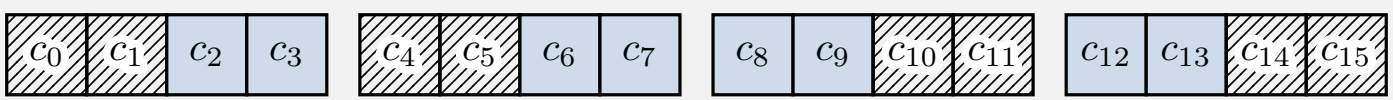
Claimed Security

- **Preimage resistance:**
  - #steps: 5
  - Security level: 256 bits
- **Collision resistance:**
  - #steps: 6 (stronger)
  - Security level: 128 bits

One step of π_{512}



Final Truncation: Remove 8 out of 16 AES columns



Haraka Round Constants

Highly Structured Round Constants

The 128-bit round constant RC_i verifies:

$$RC_i = \boxed{c_i}\boxed{c_i}\boxed{c_i}\boxed{c_i}$$

where 32-bit c_i has one bit at Position i.

$$RC_0 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; RC_1 = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; RC_2 = \begin{pmatrix} 4 & 4 & 4 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; \cdots$$

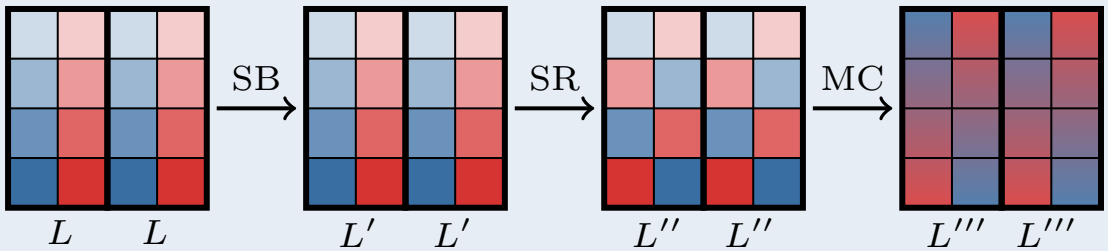
Spoiler Alert

The attacks proposed in this talk rely on this structure

Symmetries in the Keyless AES Round Function A

Classes of Size 2^{64} and 2^{32} (used in the collision attack)

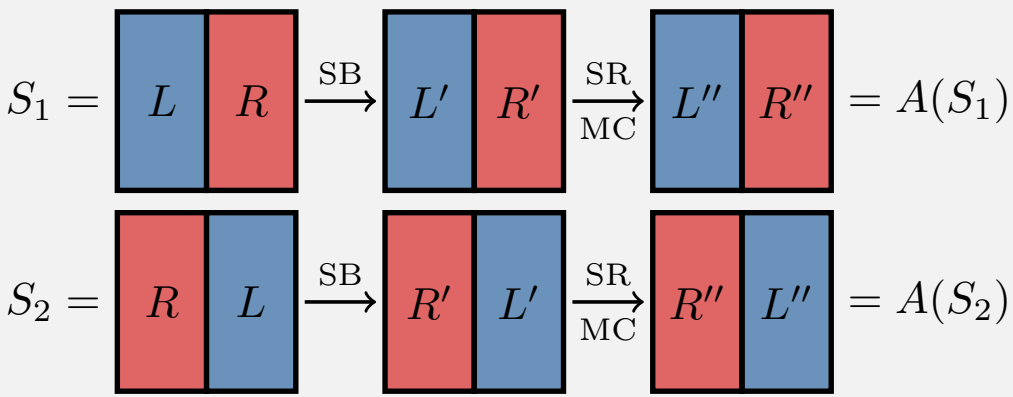
A **symmetric state** with two equal halves stays symmetric after A:



A state with four equal columns is called **strongly symmetric**

Pairs of States with Swapped Halves (used in the preimage attack)

Let (S_1, S_2) be a pair of AES states with swapped halves, then $A(S_1)$ and $A(S_2)$ also have swapped halves



Collision Attack on Haraka

General Idea

The strongly symmetric property propagates in all the Haraka components since **the round constants are strongly symmetric**

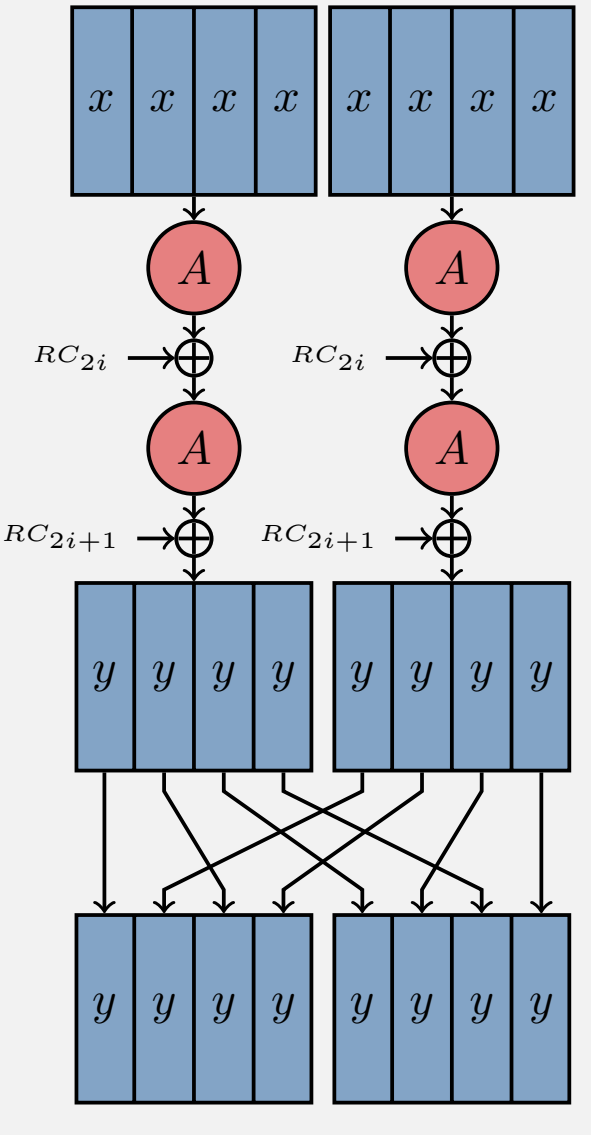
Details for Haraka-256/256

- Input: 2 AES strongly symmetric states
- Then, in each step:
  - Keyless AES maintains the property
  - Constant addition as well
  - Column reordering becomes identity
- Davies-Meyer feedforward keeps symmetry
- Hence, all output columns are equal

Notes

- Enough to collide on a 32-bit column
- Collisions after about $\mathbf{2^{16}}$ **evaluations**
- Same cost for Haraka-512/256

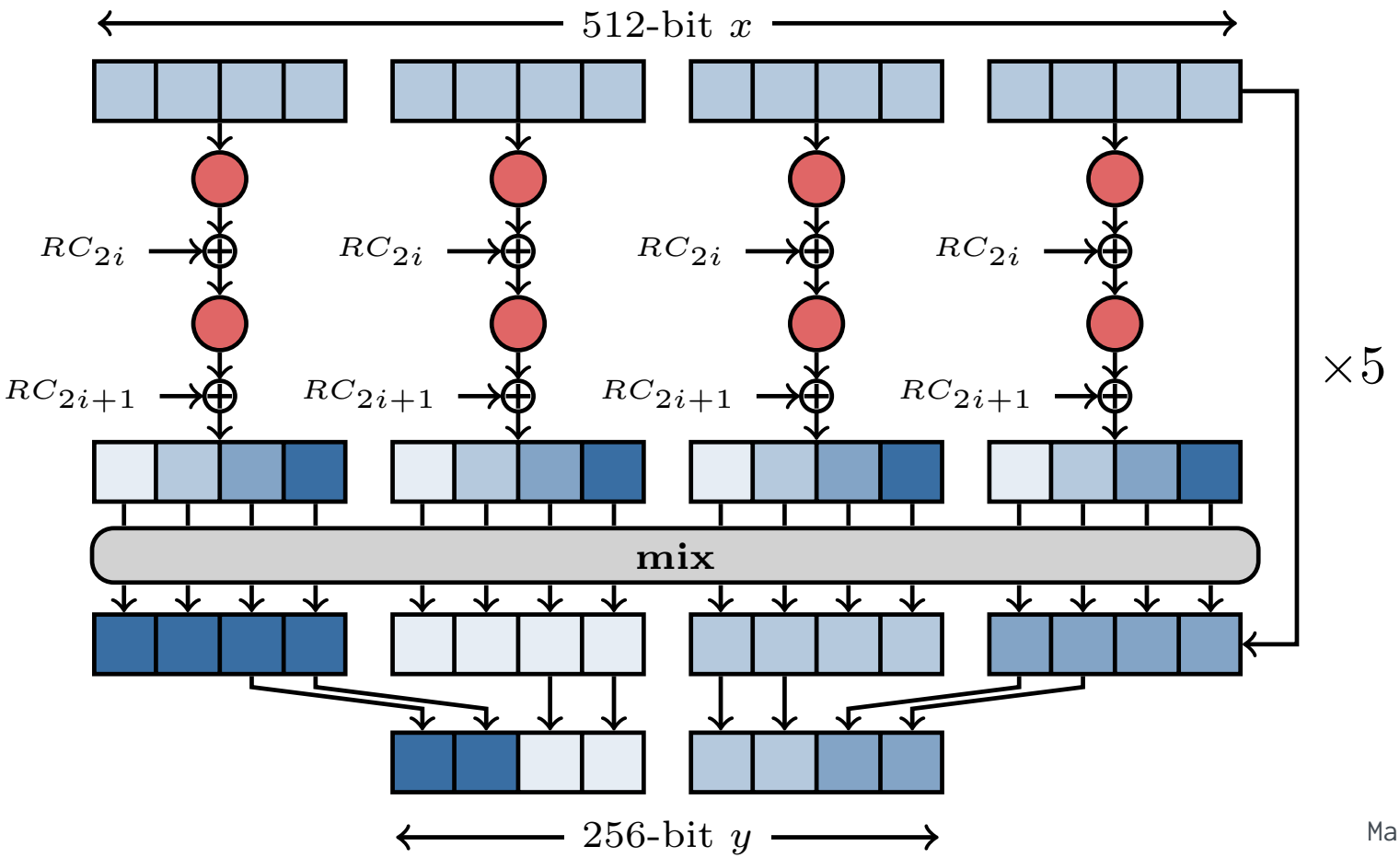
Symmetric States



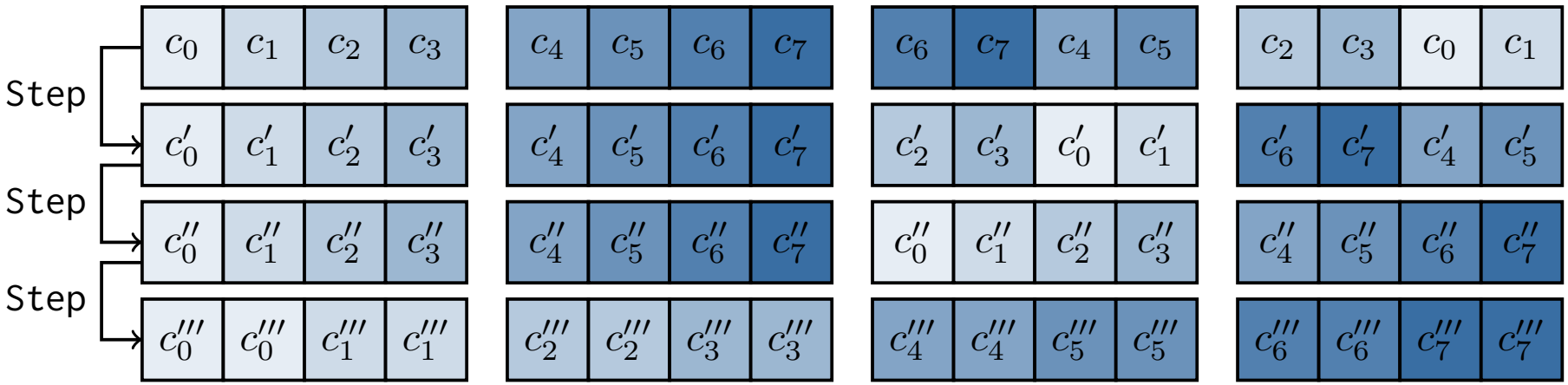
Preimage Attack on Haraka-512/256

Preimage Problem Detail and Idea

- Given y the 256-bit preimage challenge, find one 512-bit x such that Haraka-512/256$(x) = y$
- About 2^{256} solutions $\Rightarrow$ **rely on symmetry** to reduce this
- Problem too constrained for Haraka-256/256



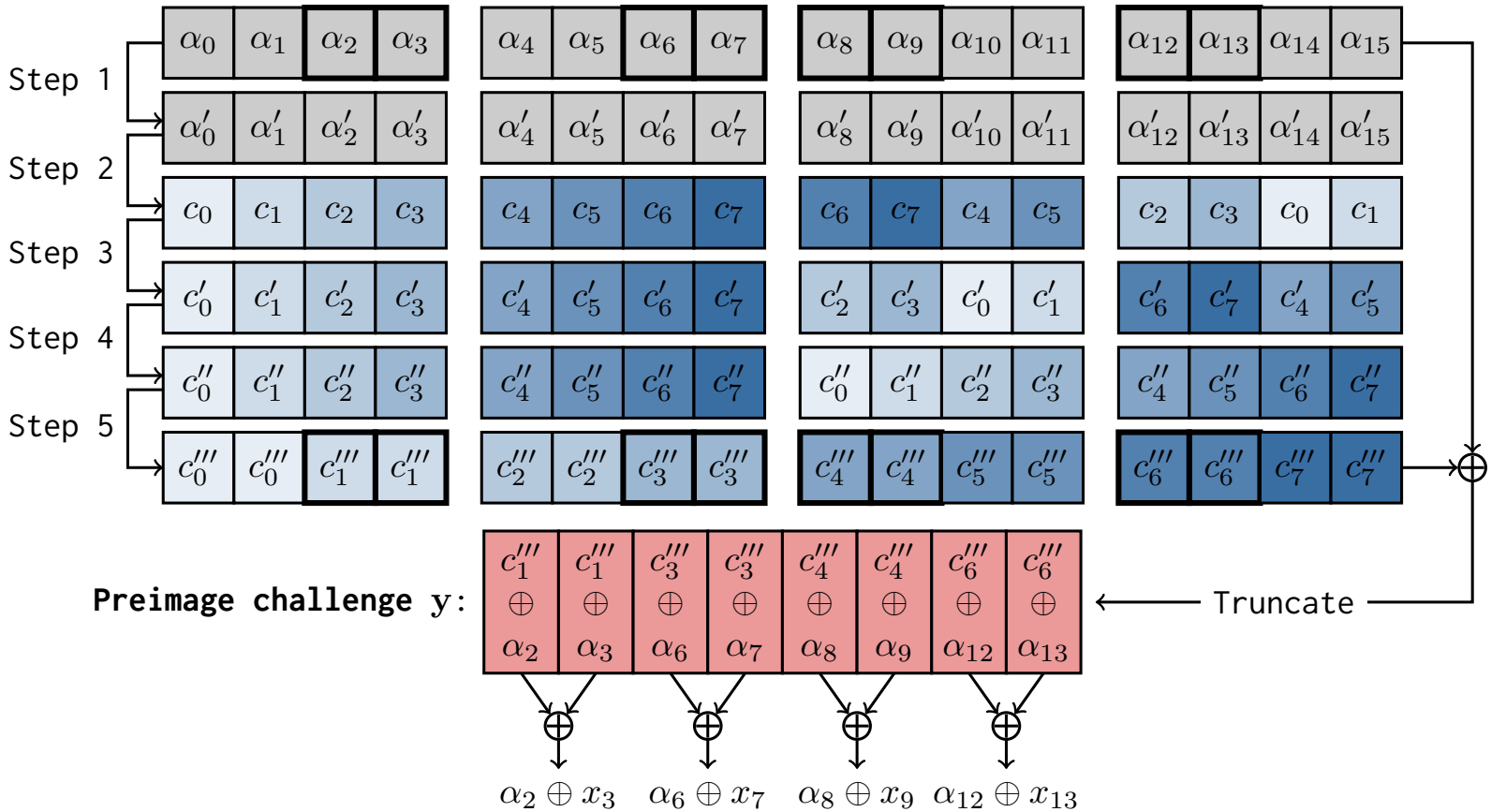
A 3-Step Symmetry Class for π_{512}



Notes

- Each variable is a 32-bit AES column
- Symmetry class extended from the one with swapped halves on AES
- Rely on the structure of the **mix** column permutation
- Size: $2^{8\times 32} = 2^{256}$ states following the 3-step symmetry
- Constrained problem: if we force the preimage to go through these 3 rounds, **only one solution expected**

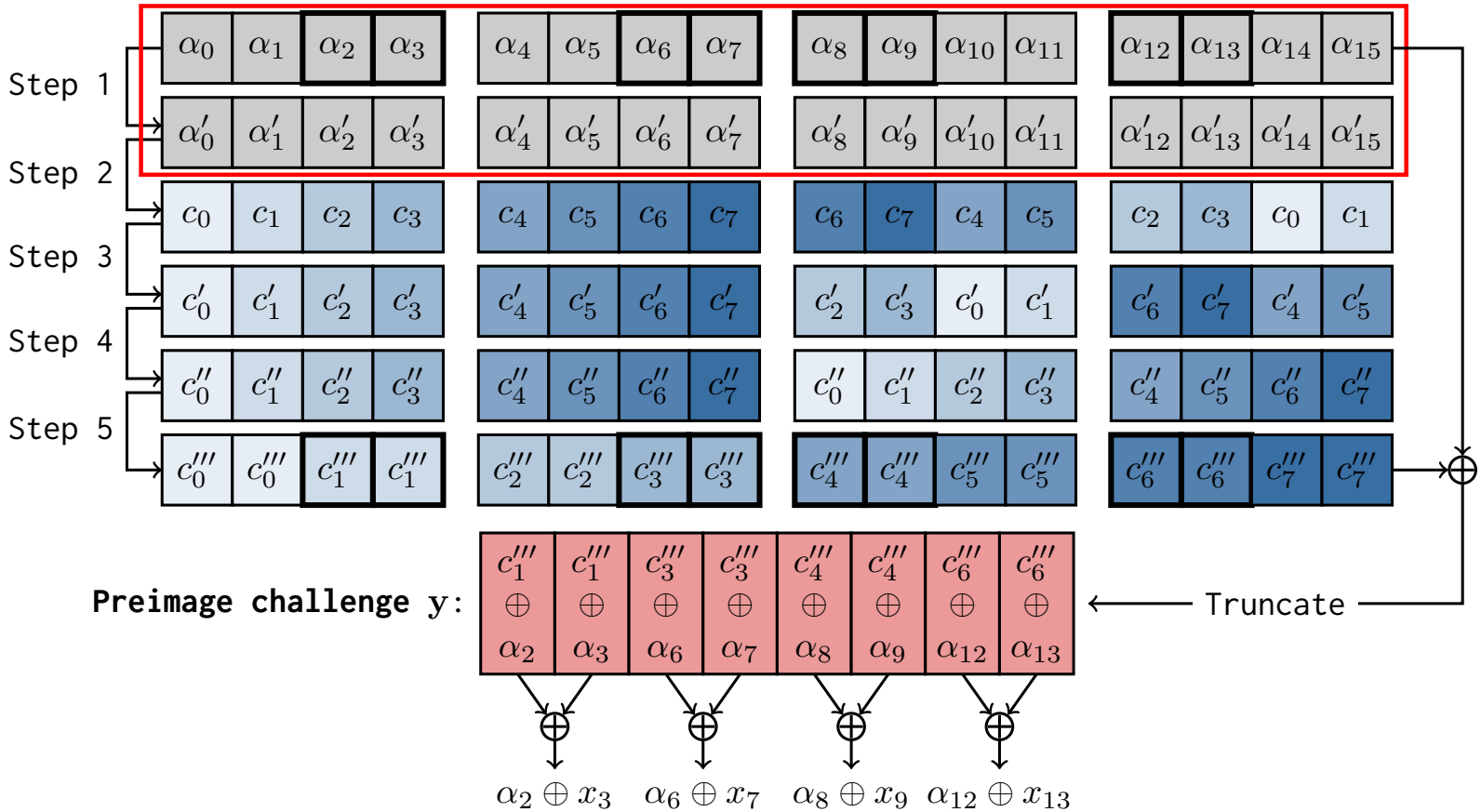
Preimage Attack Strategy I



Notes

- **If** the last 3 steps follow the symmetry $\Rightarrow$ **about 1 preimage for** y
- The challenge fixes 128 bits of the 256-bit symmetry freedom
- Hence, if an algorithm can enumerate the 2^{128} possible input states in less than 2^{256} operations, it is a **preimage attack**.

Preimage Attack Strategy II



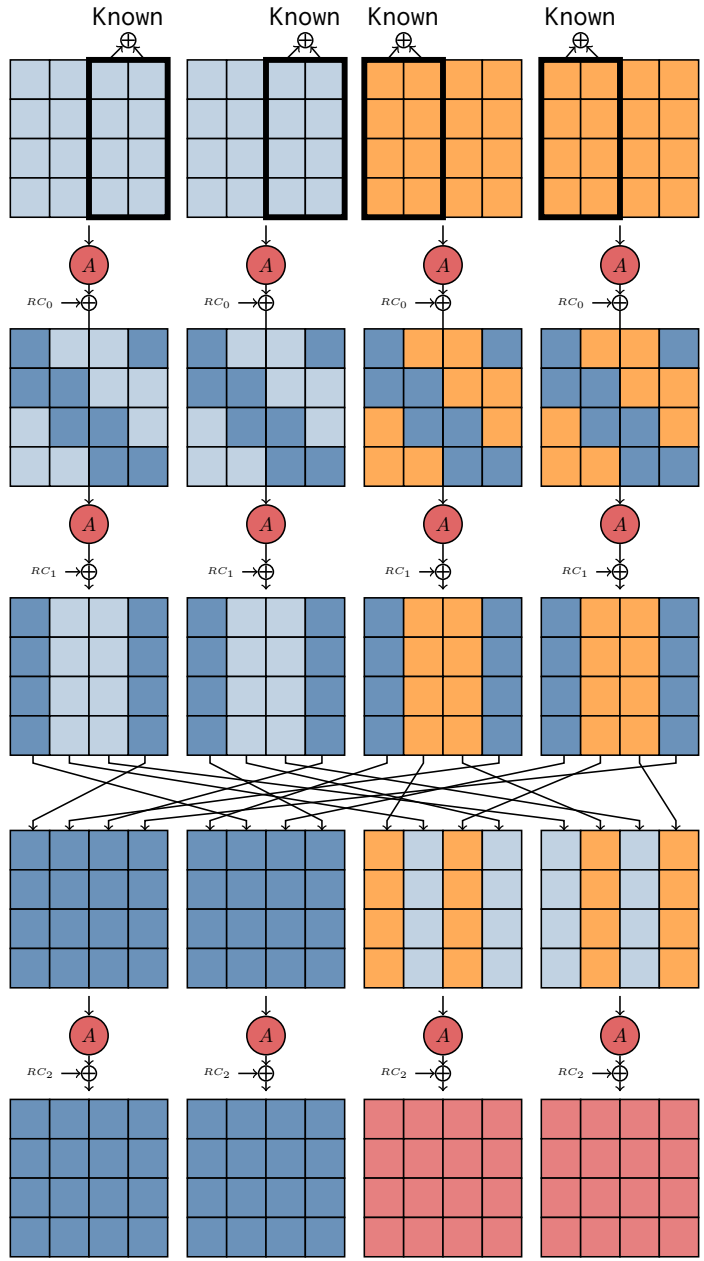
Towards an Enumeration Algorithm in 2^{192} Operations

- Focus on the steps not covered by the symmetry
- Step 2 partially inverted (formally)
- Reduction to an attack on 3-round AES with partial information on the input

Preimage Attack: Enumeration Algorithm

Algorithm (simplified)

- Due to symmetry in last 3 steps
  - at most 2^{128} values for all ■
  - at most 2^{128} values for all ■
- For all 2^{128} values of ■
  - Each of the 4 inputs states can only assume $2^{128-32-64} = 2^{32}$ values (32- and 64-bit constraints)
  - For each State $i = 0, \ldots, 3$, store the 2^{32} states in list L_i
  - For all ■ in $L_0 \times L_1$, store partial ■ in L_{01}
  - For all ■ in $L_2 \times L_3$, store partial ■ in L_{23}
  - About 1 collision between L_{01} and L_{23} $\Rightarrow$ one preimage candidate
- About 2^{128} candidates generated in about $2^{128+64} = 2^{192}$ operations



Preimage Attack on Haraka-512/256: Wrapping Up

Preimage Algorithm

- Rely on the 3-step 256-bit symmetry class
- The challenge y fixes 128 bits of the 256-bit of symmetry freedom
- Generate 2^{128} preimage candidates in 2^{192} operations
- Filter them to verify the remaining 128 bits of the preimage challenge

Conclusion

One preimage is found in about 2^{192} function evaluations,
2^{64} times faster than exhaustive search

Conclusion

Attacks

- **Collision attack**
  - Complexity: 2^{16} evaluations
  - Break 128-bit claimed security
  - Apply to any number of steps
- **Preimage attack**
  - Only works for Haraka-512/256
  - Complexity: 2^{192} function evaluations, 2^{64} memory
  - Break 256-bit claimed security

Final Remarks

- All attacks rely on a bad choice of round constant
- Designs very easy to patch
  $\Rightarrow$ Haraka v2 (see talk on Tuesday)

Conclusion

Attacks

- **Collision attack**
  - Complexity: 2^{16} evaluations
  - Break 128-bit claimed security
  - Apply to any number of steps
- **Preimage attack**
  - Only works for Haraka-512/256
  - Complexity: 2^{192} function evaluations, 2^{64} memory
  - Break 256-bit claimed security

Final Remarks

- All attacks rely on a bad choice of round constant
- Designs very easy to patch
  $\Rightarrow$ Haraka v2 (see talk on Tuesday)

Thank you for your attention!