# MD4 is Not One-Way

Gaëtan Leurent

École Normale Supérieure
Paris, France

FSE 2008

# *Hash Functions*

$$F : \{0,1\}^* \mapsto \{0,1\}^n$$

Should behave "like a random oracle".

*Collision attack*

Given $F$, find $M_1 \neq M_2$ s.t. $F(M_1) = F(M_2)$.
Ideal security: $2^{n/2}$.

*Second-preimage attack*

Given $F$ and $M_1$, find $M_2 \neq M_1$ s.t. $F(M_1) = F(M_2)$.
Ideal security: $2^n$.

*Preimage attack*

Given $F$ and $\overline{H}$, find $M$ s.t. $F(M) = \overline{H}$.
Ideal security: $2^n$.

# Hash Functions

$$F : \{0,1\}^* \mapsto \{0,1\}^n$$

Should behave "like a random oracle".

### Collision attack

Given $F$, find $M_1 \neq M_2$ s.t. $F(M_1) = F(M_2)$.
Ideal security: $2^{n/2}$.

### Second-preimage attack

Given $F$ and $M_1$, find $M_2 \neq M_1$ s.t. $F(M_1) = F(M_2)$.
Ideal security: $2^n$.

### Preimage attack

Given $F$ and $\overline{H}$, find $M$ s.t. $F(M) = \overline{H}$.
Ideal security: $2^n$.

# Hash Function Cryptanalysis

- Many papers study collision resistance...
  ... but collision attacks have limited impact.
- Preimage attacks are rather rare...
  ... but could have a devastating impact.

# Previous work

*1990* MD4 design (Rivest)

*1991* 2-round collisions (den Boer & Bosselaers – Merkle – Vaudenay)

*1996* Full collision (Dobbertin)

*1998* 2-round preimages (Dobbertin)

*2005* Very efficient collisions (Wang *et al.* – Sasaki *et al.*)

*Best attacks*

*Collisions* Complexity $2^1$ (Sasaki *et al.*)

*Preimages*
- 2 rounds: $2^{32}$ (Dobbertin)
- 2 rounds & 7 steps (De *et al.*)

# Previous work

- *1990* MD4 design (Rivest)
- *1991* 2-round collisions (den Boer & Bosselaers – Merkle – Vaudenay)
- *1996* Full collision (Dobbertin)
- *1998* 2-round preimages (Dobbertin)
- *2005* Very efficient collisions (Wang *et al.* – Sasaki *et al.*)

## Best attacks

*Collisions* Complexity $2^1$ (Sasaki *et al.*)

*Preimages*
- 2 rounds: $2^{32}$ (Dobbertin)
- 2 rounds & 7 steps (De *et al.*)

# Why bother?

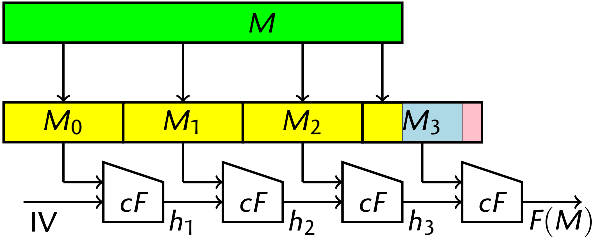
MD4 is clearly not a collision-resistant hash function, but:

- Many hash functions use a similar design:
  MD5, SHA-1, SHA-2, ...
- MD4 is believed to be one-way.
- MD4 is still in use:
  - To “encrypt” passwords in Windows NT
  - In the S/KEY one-time-password system
  - For integrity checks (rsync – eDonkey)

# The Merkle-Damgård construction

Build a hash function from a compression function.

$$cF : \{0,1\}^{n+k} \mapsto \{0,1\}^n$$
$$h_0 = \mathrm{IV}, \qquad h_{i+1} = cF(h_i, M_i)$$
$$F(M_0, M_1, ...M_{p-1}) = h_p$$




Cryptanalysis targets the compression function.

# Pseudo-preimage attack

## Pseudo-preimage attack

Given $cF$ and $\overline{H}$, find IV, $M$ s.t. $cF(\text{IV}, M) = \overline{H}$.
Ideal security: $2^n$.

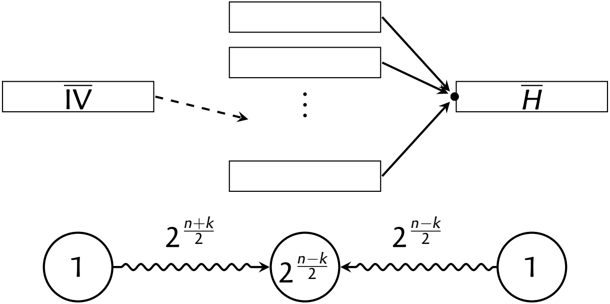
If we have a pseudo-preimage attack with complexity $2^k$,
we can build a preimage attack with complexity $2^{\frac{n+k}{2}+1}$:

# Pseudo-preimage attack

## Pseudo-preimage attack

Given $cF$ and $\overline{H}$, find IV, $M$ s.t. $cF(\text{IV}, M) = \overline{H}$.
Ideal security: $2^n$.

If we have a pseudo-preimage attack with complexity $2^k$,
we can build a preimage attack with complexity $2^{\frac{n+k}{2}+1}$:



# Our results

## MD4 compression function

- Pseudo-preimages in $2^{96}$
- Theoretical security: $2^{128}$

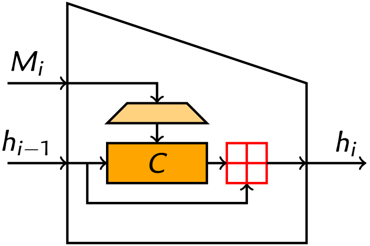
## Full MD4 hash function

- Preimages in $2^{102}$
- Theoretical security: $2^{128}$
- Message length: about 20 blocks.

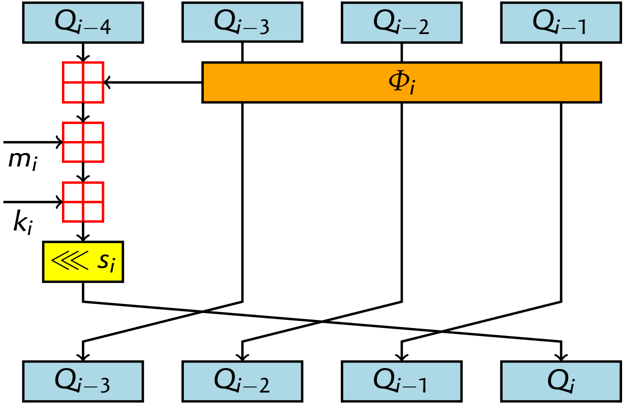
# Outline

# The MD4 hash function

- Merkle-Damgård.
  - Block size: $k = 512$ bits
  - Internal state: $n = 128$ bits
- MD Strengthening
- Davies-Meyer with a Feistel-like cipher. 3 rounds of 16 steps.



# The MD4 compression function




- $Q_i = (Q_{i-4} \boxplus \Phi_i(Q_{i-1}, Q_{i-2}, Q_{i-3}) \boxplus m_i \boxplus k_i) \lll s_i$

*In* $Q_{-4} || Q_{-1} || Q_{-2} || Q_{-3}$

*Out* $Q_{-4} \boxplus Q_{44} || Q_{-1} \boxplus Q_{47} || Q_{-2} \boxplus Q_{46} || Q_{-3} \boxplus Q_{45}$

# A System of equations

Finding a pseudo-preimage is equivalent to solving a system of equations over $\mathbb{Z}_{2^{32}}$:

$$\begin{cases} Q_i = (Q_{i-4} \boxplus \Phi_i(Q_{i-1}, Q_{i-2}, Q_{i-3}) \boxplus m_{\pi(i)} \boxplus k_i) \lll s_i \\ H_0 = Q_{-4} \boxplus Q_{44} = \overline{H}_0 \\ H_1 = Q_{-3} \boxplus Q_{45} = \overline{H}_1 \\ H_2 = Q_{-2} \boxplus Q_{46} = \overline{H}_2 \\ H_3 = Q_{-1} \boxplus Q_{47} = \overline{H}_3 \end{cases}$$

- 52 equations.
- 68 unknowns: $Q_{-3} \dots Q_{47}$ and $m_0 \dots m_{15}$.

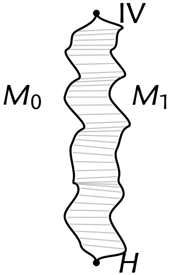
# Outline

# Starting point

- MD4 is badly broken by differential attacks.
- Can we use differential tools to build preimages?

# Differential attacks

Collision attack:




Use a differential pair:

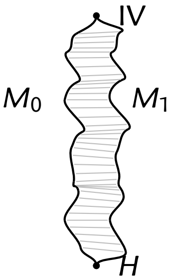
$$M_1 = M_0 + \Delta$$

- Select $M_0$
- Test if $H(M_0) = H(M_1)$

Break if $t/p \ll 2^{n/2}$

# Differential attacks

Collision attack:




Use a differential pair:

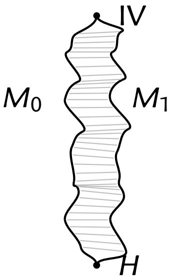
$$M_1 = M_0 + \Delta$$

- Select $M_0$
- Test if $H(M_0) = H(M_1)$

Break if $t/p \ll 2^{n/2}$

# *Differential attacks*

Collision attack:



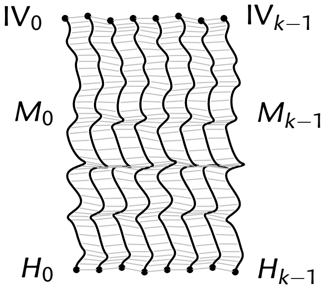

Use a differential pair:

$$M_1 = M_0 + \Delta$$

- Select $M_0$
- Test if $H(M_0) = H(M_1)$

Break if $t/p \ll 2^{n/2}$

Preimage attack:




Use a differential set:

$$(M_i, \mathsf{IV}_i) = f_i(M_0, \mathsf{IV}_0)$$

- Select $(M_0, \mathsf{IV}_0)$
- Test if $\overline{H} \in \{H_i\}$

Break if $t \ll 2^k$

# Differential attacks

Collision attack:

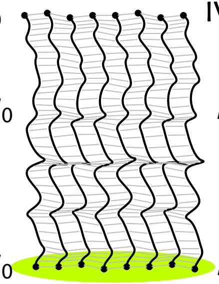

Use a differential pair:

$$M_1 = M_0 + \Delta$$

- Select $M_0$
- Test if $H(M_0) = H(M_1)$

Break if $t/p \ll 2^{n/2}$

Preimage attack:




Use a differential set:

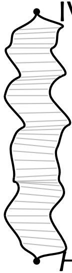
$$(M_i, \mathsf{IV}_i) = f_i(M_0, \mathsf{IV}_0)$$

- Select $(M_0, \mathsf{IV}_0)$
- Test if $\overline{H} \in \{H_i\}$

Break if $t \ll 2^k$

# Differential attacks

Collision attack:



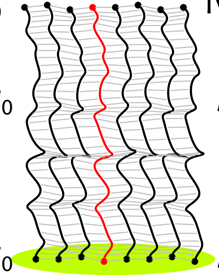

Use a differential pair:

$$M_1 = M_0 + \Delta$$

- Select $M_0$
- Test if $H(M_0) = H(M_1)$

Break if $t/p \ll 2^{n/2}$

Preimage attack:




Use a differential set:

$$(M_i, \mathsf{IV}_i) = f_i(M_0, \mathsf{IV}_0)$$

- Select $(M_0, \mathsf{IV}_0)$
- Test if $\overline{H} \in \{H_i\}$

Break if $t \ll 2^k$

# MD4 Differential Property

In the first and second rounds, the round function can absorb one difference:

## First round

- $\mathsf{IF}(x, \mathbf{C}, \mathbf{C}) = \mathbf{C}$
- $\mathsf{IF}(\mathbf{0}, x, \mathbf{C}) = \mathbf{C}$
- $\mathsf{IF}(\mathbf{1}, \mathbf{C}, x) = \mathbf{C}$

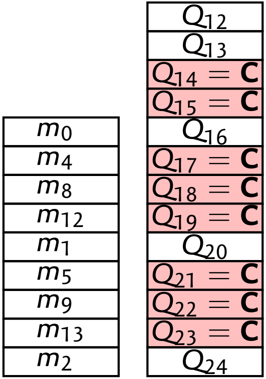
## Second round

- $\mathsf{MAJ}(x, \mathbf{C}, \mathbf{C}) = \mathbf{C}$
- $\mathsf{MAJ}(\mathbf{C}, x, \mathbf{C}) = \mathbf{C}$
- $\mathsf{MAJ}(\mathbf{C}, \mathbf{C}, x) = \mathbf{C}$

We use this property to build our differential path.

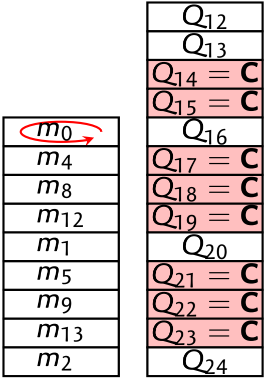
# MD4 Absorption: second round

- Pick a message with good $Q_i$'s (fix **C**)
- Modify $m_0$



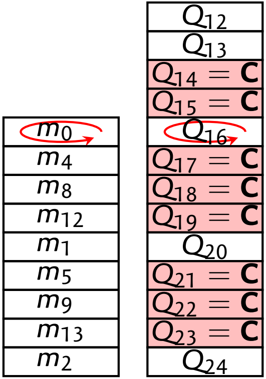
# MD4 Absorption: second round

- Pick a message with good $Q_i$'s (fix **C**)
- Modify $m_0$



# MD4 Absorption: second round

- Pick a message with good $Q_i$'s (fix $\mathbf{C}$)
- Modify $m_0$



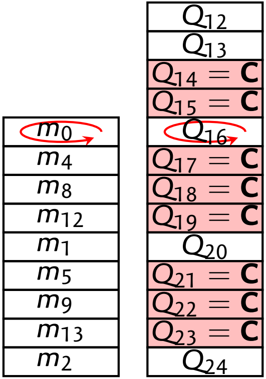

*Step 16*

$$Q_{16} = (Q_{12} \boxplus \mathrm{MAJ}(\mathbf{C}\ \ , \mathbf{C}\ \ , Q_{13}) \boxplus m_0) \lll 3$$

$$\mathrm{MAJ}(\mathbf{C}\ \ , \mathbf{C}\ \ , Q_{13}) = \mathbf{C}$$

# MD4 Absorption: second round

- Pick a message with good $Q_i$'s (fix $\mathbf{C}$)
- Modify $m_0$



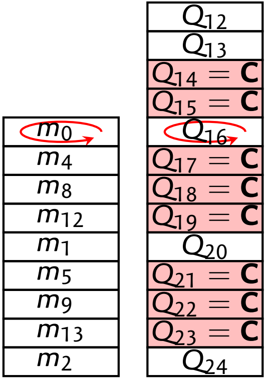

## Step 17

$$Q_{17} = (Q_{13} \boxplus \mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) \boxplus m_4) \lll 7$$

$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) = \mathbf{C}$$
$$\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) = \mathbf{C}$$

# MD4 Absorption: second round

- Pick a message with good $Q_i$'s (fix $\mathbf{C}$)
- Modify $m_0$



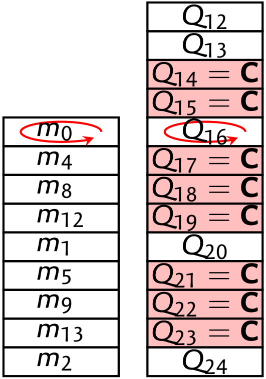

*Step 18*

$$Q_{18} = (\mathbf{C} \boxplus \mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) \boxplus m_8) \lll 11$$

$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) = \mathbf{C}$$
$$\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) = \mathbf{C}$$

# MD4 Absorption: second round

- Pick a message with good $Q_i$'s (fix $\mathbf{C}$)
- Modify $m_0$



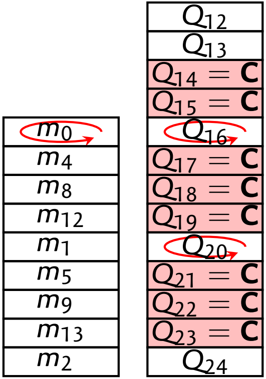

*Step 19*

$$Q_{19} = (\mathbf{C} \boxplus \mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{16}) \boxplus m_{12}) \lll 19$$

$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) = \mathbf{C}$$
$$\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{16}) = \mathbf{C}$$

# MD4 Absorption: second round

- Pick a message with good $Q_i$'s (fix $\mathbf{C}$)
- Modify $m_0$




*Step 20*

$$Q_{20} = (Q_{16} \boxplus \mathrm{MAJ}(\mathbf{C}, \mathbf{C}, \mathbf{C}) \boxplus m_1) \lll 3$$

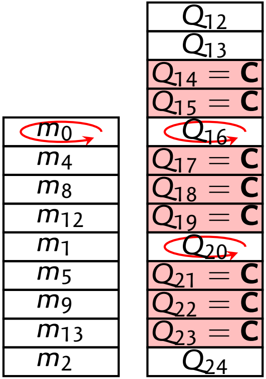
$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) = \mathbf{C}$$
$$\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{16}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, \mathbf{C}) = \mathbf{C}$$

# *MD4 Absorption: second round*

- Pick a message with good $Q_i$'s (fix **C**)
- Modify $m_0$

*Step 21*

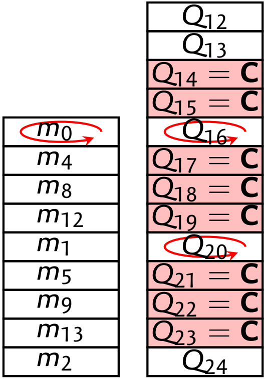
$$Q_{21} = (\mathbf{C} \boxplus \mathrm{MAJ}(Q_{20}, \mathbf{C}, \mathbf{C}) \boxplus m_5) \lll 7$$




$$\begin{aligned}
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{16}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{20}, \mathbf{C}, \mathbf{C}) &= \mathbf{C}
\end{aligned}$$

# MD4 Absorption: second round

- Pick a message with good $Q_i$'s (fix $\mathbf{C}$)
- Modify $m_0$




### Step 22

$$Q_{22} = (\mathbf{C} \boxplus \mathrm{MAJ}(\mathbf{C}, Q_{20}, \mathbf{C}) \boxplus m_9) \lll 11$$

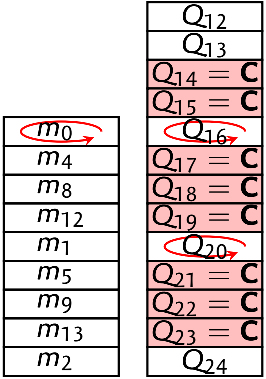
$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) = \mathbf{C}$$
$$\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{16}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, \mathbf{C}) = \mathbf{C}$$
$$\mathrm{MAJ}(Q_{20}, \mathbf{C}, \mathbf{C}) = \mathbf{C}$$
$$\mathrm{MAJ}(\mathbf{C}, Q_{20}, \mathbf{C}) = \mathbf{C}$$

# MD4 Absorption: second round

- Pick a message with good $Q_i$'s (fix **C**)
- Modify $m_0$

### Step 23

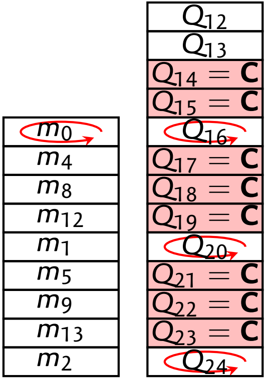
$$Q_{23} = (\mathbf{C} \boxplus \mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{20}) \boxplus m_{13}) \lll 19$$




$$\begin{aligned}
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{16}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{20}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, Q_{20}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{20}) &= \mathbf{C}
\end{aligned}$$

# MD4 Absorption: second round

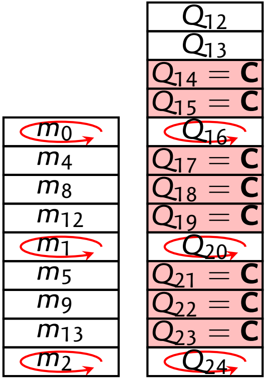
- Pick a message with good $Q_i$'s (fix $\mathbf{C}$)
- Modify $m_0$
- Only $Q_{16}$, $Q_{20}$, $Q_{24}$, ... are affected.




$$
\begin{aligned}
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{16}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{20}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, Q_{20}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{20}) &= \mathbf{C} \\
&\dots
\end{aligned}
$$

# MD4 Absorption: second round

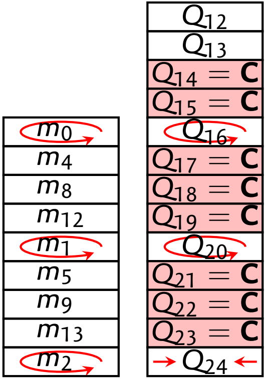
- Pick a message with good $Q_i$'s (fix **C**)
- Modify $m_0$
- Only $Q_{16}$, $Q_{20}$, $Q_{24}$, ... are affected.
- We can also modify $m_1$, $m_2$, ...




$$
\begin{aligned}
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{16}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{20}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, Q_{20}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{20}) &= \mathbf{C} \\
\ldots
\end{aligned}
$$

# MD4 Absorption: second round

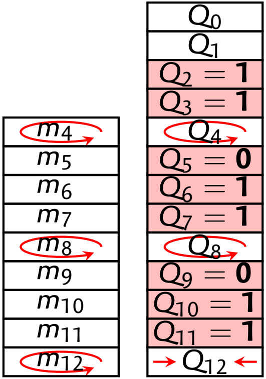
- Pick a message with good $Q_i$'s (fix $\mathbf{C}$)
- Modify $m_0$
- Only $Q_{16}$, $Q_{20}$, $Q_{24}$, ... are affected.
- We can also modify $m_1$, $m_2$, ...
- Local collision if we force $Q_{24}$.




$$
\begin{aligned}
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{13}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{16}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, Q_{16}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{16}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(Q_{20}, \mathbf{C}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, Q_{20}, \mathbf{C}) &= \mathbf{C} \\
\mathrm{MAJ}(\mathbf{C}, \mathbf{C}, Q_{20}) &= \mathbf{C} \\
&\cdots
\end{aligned}
$$

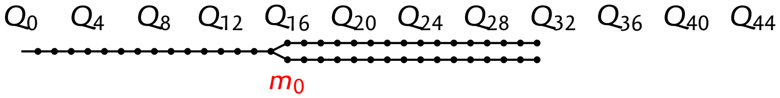
# MD4 Absorption: first round

- Pick a message with good $Q_i$'s
- Modify $m_4$
- Only $Q_4$, $Q_8$, $Q_{12}$, ... are affected.
- We can also modify $m_8$, $m_{12}$, ...
- Local collision if we force $Q_{12}$.




$$
\begin{array}{l}
\mathrm{IF}(\mathbf{1}, \mathbf{1}, Q_1) = \mathbf{1} \\
\mathrm{IF}(Q_4, \mathbf{1}, \mathbf{1}) = \mathbf{1} \\
\mathrm{IF}(\mathbf{0}, Q_4, \mathbf{1}) = \mathbf{1} \\
\mathrm{IF}(\mathbf{1}, \mathbf{0}, Q_4) = \mathbf{0} \\
\mathrm{IF}(\mathbf{1}, \mathbf{1}, \mathbf{0}) = \mathbf{1} \\
\mathrm{IF}(Q_8, \mathbf{1}, \mathbf{1}) = \mathbf{1} \\
\mathrm{IF}(\mathbf{0}, Q_8, \mathbf{1}) = \mathbf{1} \\
\mathrm{IF}(\mathbf{1}, \mathbf{0}, Q_8) = \mathbf{0} \\
\cdots
\end{array}
$$

# The differential path

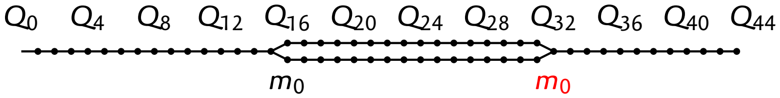



- Introduce the difference at step 16 ($m_0$).
- Cancel the difference at step 32 ($m_0$).
- Use $m_3$ as a degree of freedom.
- $m_0$ and $m_3$ are used at the very beginning and the very end.

We have $2^{32}$ messages $(m_0, m_3)$ with only 8 free steps.

- We control round 2 thanks to the conditions on the $Q_i$'s.
- We skip round 1 and 3 thanks to the position of the differences.

# The differential path

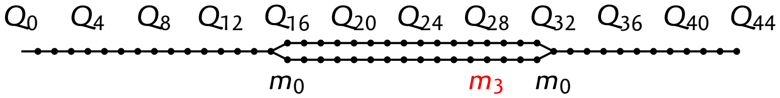



- Introduce the difference at step 16 ($m_0$).
- Cancel the difference at step 32 ($m_0$).
- Use $m_3$ as a degree of freedom.
- $m_0$ and $m_3$ are used at the very beginning and the very end.

We have $2^{32}$ messages $(m_0, m_3)$ with only 8 free steps.

- We control round 2 thanks to the conditions on the $Q_i$'s.
- We skip round 1 and 3 thanks to the position of the differences.

# The differential path

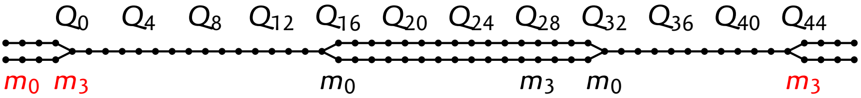



- Introduce the difference at step 16 ($m_0$).
- Cancel the difference at step 32 ($m_0$).
- Use $m_3$ as a degree of freedom.
- $m_0$ and $m_3$ are used at the very beginning and the very end.

We have $2^{32}$ messages $(m_0, m_3)$ with only 8 free steps.

- We control round 2 thanks to the conditions on the $Q_i$'s.
- We skip round 1 and 3 thanks to the position of the differences.

# The differential path

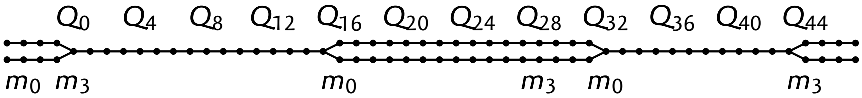



- Introduce the difference at step 16 ($m_0$).
- Cancel the difference at step 32 ($m_0$).
- Use $m_3$ as a degree of freedom.
- $m_0$ and $m_3$ are used at the very beginning and the very end.

We have $2^{32}$ messages $(m_0, m_3)$ with only 8 free steps.

- We control round 2 thanks to the conditions on the $Q_i$'s.
- We skip round 1 and 3 thanks to the position of the differences.

# The differential path



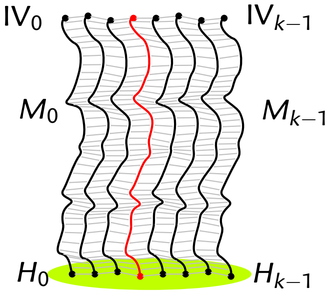

- Introduce the difference at step 16 ($m_0$).
- Cancel the difference at step 32 ($m_0$).
- Use $m_3$ as a degree of freedom.
- $m_0$ and $m_3$ are used at the very beginning and the very end.

We have $2^{32}$ messages $(m_0, m_3)$ with only 8 free steps.

- We control round 2 thanks to the conditions on the $Q_i$'s.
- We skip round 1 and 3 thanks to the position of the differences.

# Overview

Preimage attack:

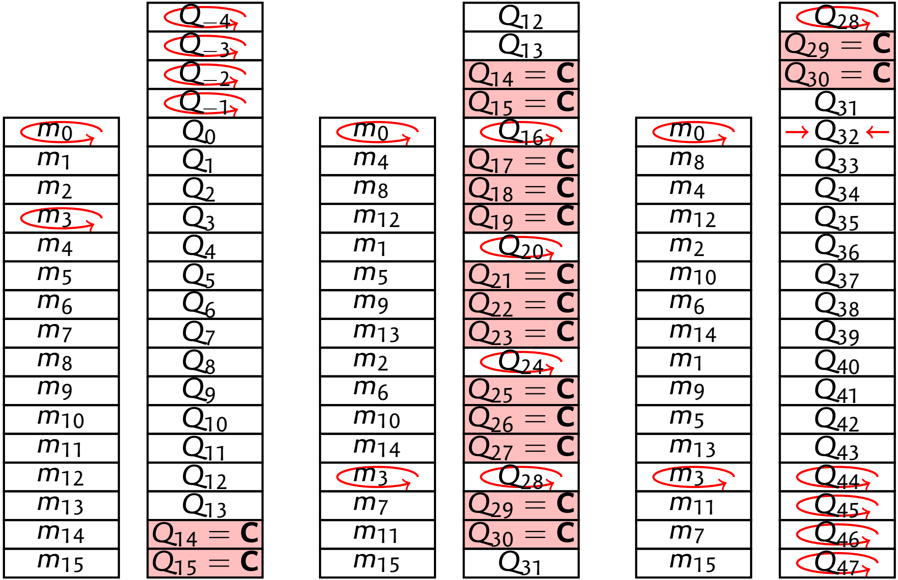



Use a differential set:

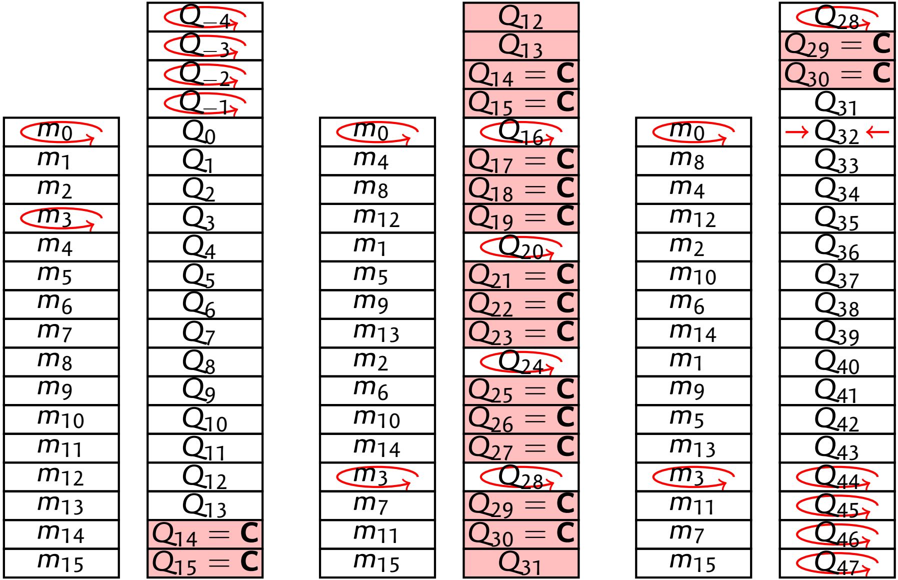
$$(M_i, IV_i) = f_i(M_0, IV_0)$$

- Select $(M_0, IV_0)$
- Test if $\overline{H} \in \{H_i\}$

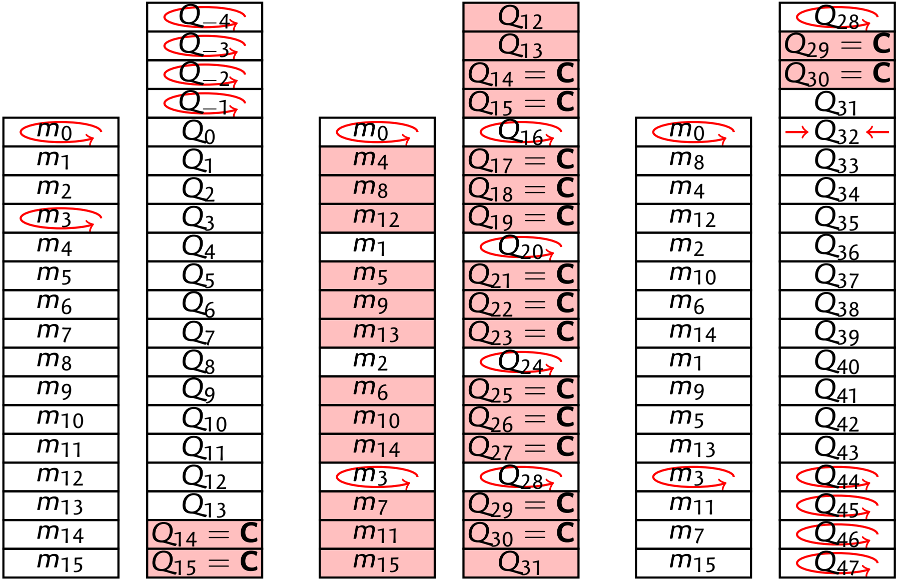
- Find an initial message $(M_0, IV_0)$ with some $Q_i$ fixed.
- Use the freedom in $m_1$ and $m_2$ to simplify the equations: related message.
- We have a differential set of $2^{32}$ messages $(m_0, m_3)$.
- Study the first and last steps to test if one message yields $\overline{H}$.



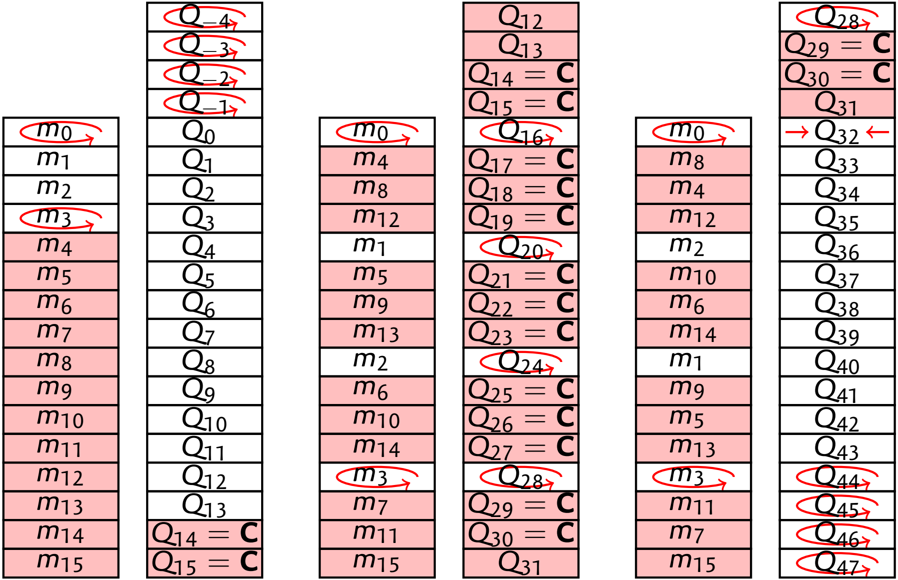
$m_0$
$m_1$
$m_2$
$m_3$
$m_4$
$m_5$
$m_6$
$m_7$
$m_8$
$m_9$
$m_{10}$
$m_{11}$
$m_{12}$
$m_{13}$
$m_{14}$
$m_{15}$
$Q_{-4}$
$Q_{-3}$
$Q_{-2}$
$Q_{-1}$
$Q_0$
$Q_1$
$Q_2$
$Q_3$
$Q_4$
$Q_5$
$Q_6$
$Q_7$
$Q_8$
$Q_9$
$Q_{10}$
$Q_{11}$
$Q_{12}$
$Q_{13}$
$Q_{14} = \mathbf{C}$
$Q_{15} = \mathbf{C}$
$m_0$
$m_4$
$m_8$
$m_{12}$
$m_1$
$m_5$
$m_9$
$m_{13}$
$m_2$
$m_6$
$m_{10}$
$m_{14}$
$m_3$
$m_7$
$m_{11}$
$m_{15}$
$Q_{12}$
$Q_{13}$
$Q_{14} = \mathbf{C}$
$Q_{15} = \mathbf{C}$
$Q_{16}$
$Q_{17} = \mathbf{C}$
$Q_{18} = \mathbf{C}$
$Q_{19} = \mathbf{C}$
$Q_{20}$
$Q_{21} = \mathbf{C}$
$Q_{22} = \mathbf{C}$
$Q_{23} = \mathbf{C}$
$Q_{24}$
$Q_{25} = \mathbf{C}$
$Q_{26} = \mathbf{C}$
$Q_{27} = \mathbf{C}$
$Q_{28}$
$Q_{29} = \mathbf{C}$
$Q_{30} = \mathbf{C}$
$Q_{31}$
$m_0$
$m_8$
$m_4$
$m_{12}$
$m_2$
$m_{10}$
$m_6$
$m_{14}$
$m_1$
$m_9$
$m_5$
$m_{13}$
$m_3$
$m_{11}$
$m_7$
$m_{15}$
$Q_{28}$
$Q_{29} = \mathbf{C}$
$Q_{30} = \mathbf{C}$
$Q_{31}$
$\rightarrow Q_{32} \leftarrow$
$Q_{33}$
$Q_{34}$
$Q_{35}$
$Q_{36}$
$Q_{37}$
$Q_{38}$
$Q_{39}$
$Q_{40}$
$Q_{41}$
$Q_{42}$
$Q_{43}$
$Q_{44}$
$Q_{45}$
$Q_{46}$
$Q_{47}$



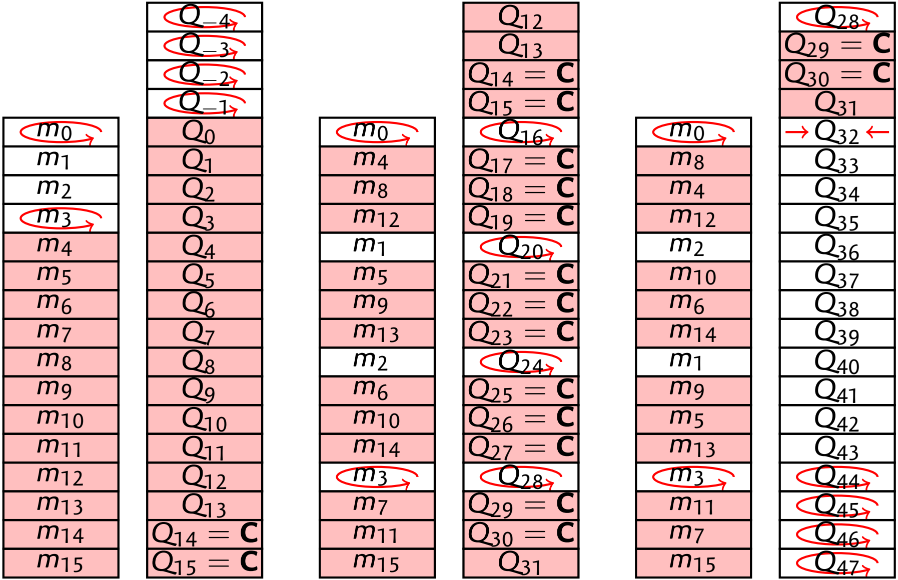
$m_0$ $m_1$ $m_2$ $m_3$ $m_4$ $m_5$ $m_6$ $m_7$ $m_8$ $m_9$ $m_{10}$ $m_{11}$ $m_{12}$ $m_{13}$ $m_{14}$ $m_{15}$
$Q_{-4}$ $Q_{-3}$ $Q_{-2}$ $Q_{-1}$ $Q_0$ $Q_1$ $Q_2$ $Q_3$ $Q_4$ $Q_5$ $Q_6$ $Q_7$ $Q_8$ $Q_9$ $Q_{10}$ $Q_{11}$ $Q_{12}$ $Q_{13}$ $Q_{14} = \mathbf{C}$ $Q_{15} = \mathbf{C}$
$m_0$ $m_4$ $m_8$ $m_{12}$ $m_1$ $m_5$ $m_9$ $m_{13}$ $m_2$ $m_6$ $m_{10}$ $m_{14}$ $m_3$ $m_7$ $m_{11}$ $m_{15}$
$Q_{12}$ $Q_{13}$ $Q_{14} = \mathbf{C}$ $Q_{15} = \mathbf{C}$ $Q_{16}$ $Q_{17} = \mathbf{C}$ $Q_{18} = \mathbf{C}$ $Q_{19} = \mathbf{C}$ $Q_{20}$ $Q_{21} = \mathbf{C}$ $Q_{22} = \mathbf{C}$ $Q_{23} = \mathbf{C}$ $Q_{24}$ $Q_{25} = \mathbf{C}$ $Q_{26} = \mathbf{C}$ $Q_{27} = \mathbf{C}$ $Q_{28}$ $Q_{29} = \mathbf{C}$ $Q_{30} = \mathbf{C}$ $Q_{31}$
$m_0$ $m_8$ $m_4$ $m_{12}$ $m_2$ $m_{10}$ $m_6$ $m_{14}$ $m_1$ $m_9$ $m_5$ $m_{13}$ $m_3$ $m_{11}$ $m_7$ $m_{15}$
$Q_{28}$ $Q_{29} = \mathbf{C}$ $Q_{30} = \mathbf{C}$ $Q_{31}$ $Q_{32}$ $Q_{33}$ $Q_{34}$ $Q_{35}$ $Q_{36}$ $Q_{37}$ $Q_{38}$ $Q_{39}$ $Q_{40}$ $Q_{41}$ $Q_{42}$ $Q_{43}$ $Q_{44}$ $Q_{45}$ $Q_{46}$ $Q_{47}$

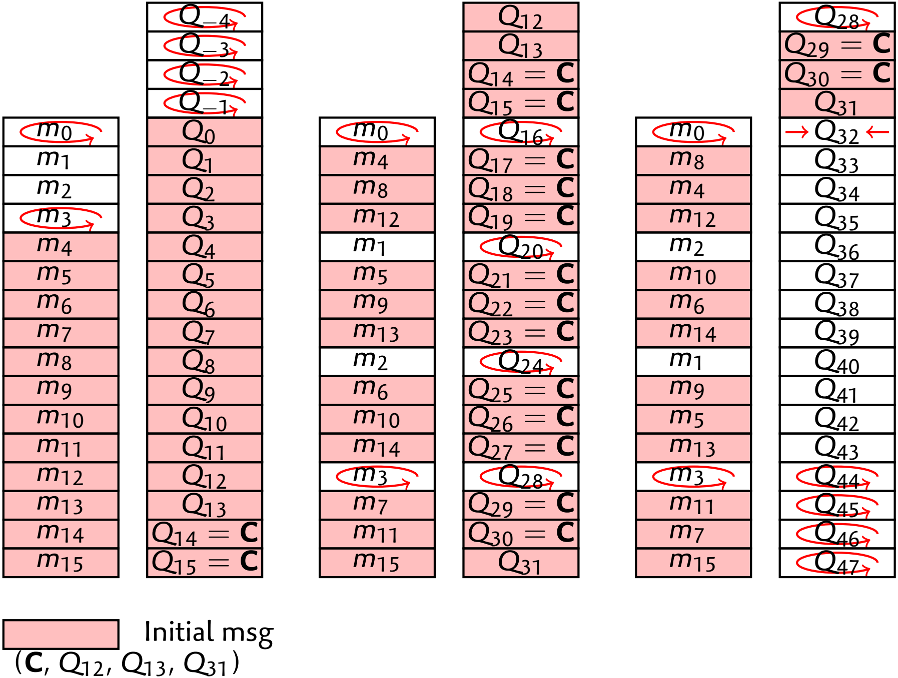


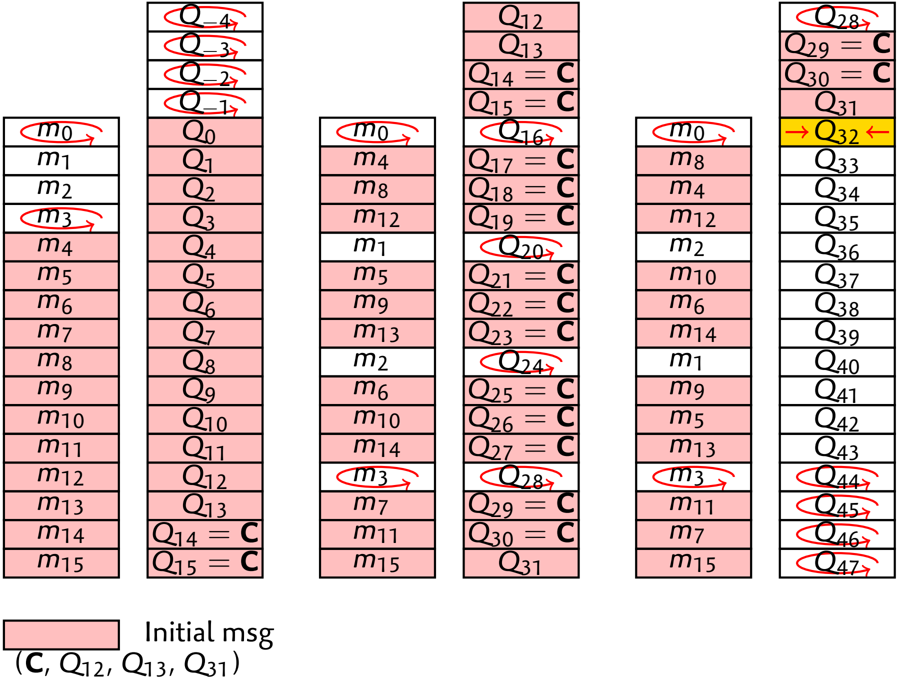
m0 m1 m2 m3 m4 m5 m6 m7 m8 m9 m10 m11 m12 m13 m14 m15
Q−4 Q−3 Q−2 Q−1 Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10 Q11 Q12 Q13
Q14 = C
Q15 = C
m0 m4 m8 m12 m1 m5 m9 m13 m2 m6 m10 m14 m3 m7 m11 m15
Q12 Q13
Q14 = C
Q15 = C
Q16
Q17 = C
Q18 = C
Q19 = C
Q20
Q21 = C
Q22 = C
Q23 = C
Q24
Q25 = C
Q26 = C
Q27 = C
Q28
Q29 = C
Q30 = C
Q31
m0 m8 m4 m12 m2 m10 m6 m14 m1 m9 m5 m13 m3 m11 m7 m15
Q28
Q29 = C
Q30 = C
Q31 Q32 Q33 Q34 Q35 Q36 Q37 Q38 Q39 Q40 Q41 Q42 Q43 Q44 Q45 Q46 Q47



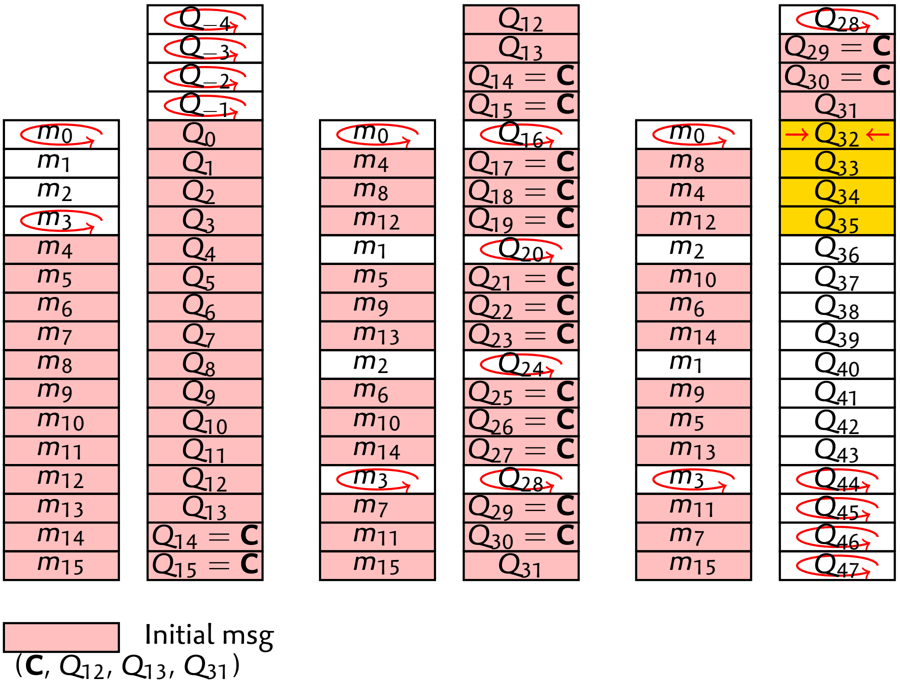
m0
m1
m2
m3
m4
m5
m6
m7
m8
m9
m10
m11
m12
m13
m14
m15
Q−4
Q−3
Q−2
Q−1
Q0
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
Q9
Q10
Q11
Q12
Q13
Q14 = C
Q15 = C
m0
m4
m8
m12
m1
m5
m9
m13
m2
m6
m10
m14
m3
m7
m11
m15
Q12
Q13
Q14 = C
Q15 = C
Q16
Q17 = C
Q18 = C
Q19 = C
Q20
Q21 = C
Q22 = C
Q23 = C
Q24
Q25 = C
Q26 = C
Q27 = C
Q28
Q29 = C
Q30 = C
Q31
m0
m8
m4
m12
m2
m10
m6
m14
m1
m9
m5
m13
m3
m11
m7
m15
Q28
Q29 = C
Q30 = C
Q31
Q32
Q33
Q34
Q35
Q36
Q37
Q38
Q39
Q40
Q41
Q42
Q43
Q44
Q45
Q46
Q47


m0 m1 m2 m3 m4 m5 m6 m7 m8 m9 m10 m11 m12 m13 m14 m15
Q−4 Q−3 Q−2 Q−1 Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10 Q11 Q12 Q13 Q14 = C Q15 = C
m0 m4 m8 m12 m1 m5 m9 m13 m2 m6 m10 m14 m3 m7 m11 m15
Q12 Q13 Q14 = C Q15 = C Q16 Q17 = C Q18 = C Q19 = C Q20 Q21 = C Q22 = C Q23 = C Q24 Q25 = C Q26 = C Q27 = C Q28 Q29 = C Q30 = C Q31
m0 m8 m4 m12 m2 m10 m6 m14 m1 m9 m5 m13 m3 m11 m7 m15
Q28 Q29 = C Q30 = C Q31 Q32 Q33 Q34 Q35 Q36 Q37 Q38 Q39 Q40 Q41 Q42 Q43 Q44 Q45 Q46 Q47

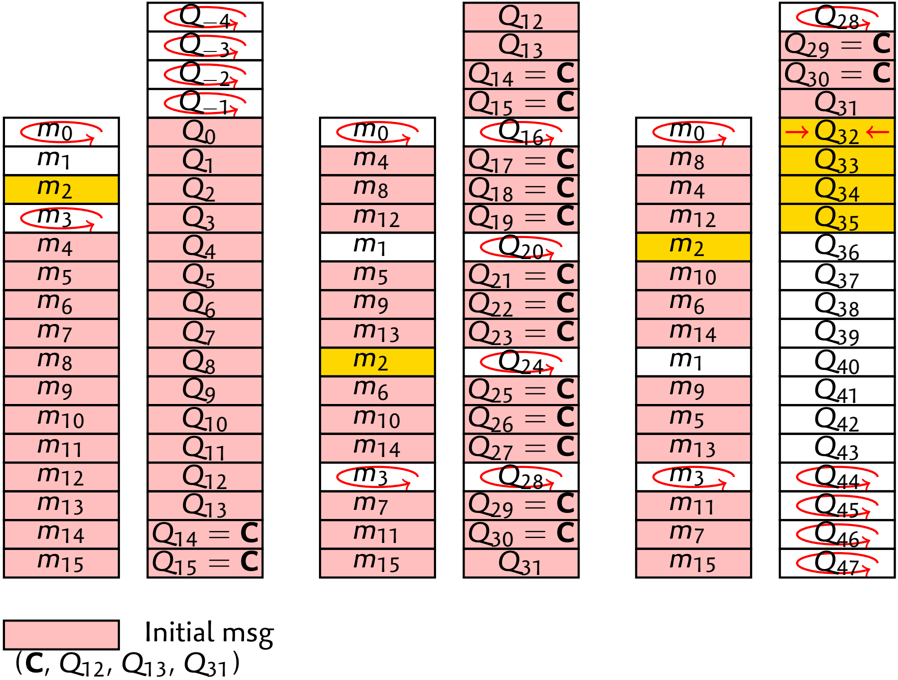

$m_0$ $m_1$ $m_2$ $m_3$ $m_4$ $m_5$ $m_6$ $m_7$ $m_8$ $m_9$ $m_{10}$ $m_{11}$ $m_{12}$ $m_{13}$ $m_{14}$ $m_{15}$
$Q_{-4}$ $Q_{-3}$ $Q_{-2}$ $Q_{-1}$ $Q_0$ $Q_1$ $Q_2$ $Q_3$ $Q_4$ $Q_5$ $Q_6$ $Q_7$ $Q_8$ $Q_9$ $Q_{10}$ $Q_{11}$ $Q_{12}$ $Q_{13}$ $Q_{14} = \mathbf{C}$ $Q_{15} = \mathbf{C}$
$m_0$ $m_4$ $m_8$ $m_{12}$ $m_1$ $m_5$ $m_9$ $m_{13}$ $m_2$ $m_6$ $m_{10}$ $m_{14}$ $m_3$ $m_7$ $m_{11}$ $m_{15}$
$Q_{12}$ $Q_{13}$ $Q_{14} = \mathbf{C}$ $Q_{15} = \mathbf{C}$ $Q_{16}$ $Q_{17} = \mathbf{C}$ $Q_{18} = \mathbf{C}$ $Q_{19} = \mathbf{C}$ $Q_{20}$ $Q_{21} = \mathbf{C}$ $Q_{22} = \mathbf{C}$ $Q_{23} = \mathbf{C}$ $Q_{24}$ $Q_{25} = \mathbf{C}$ $Q_{26} = \mathbf{C}$ $Q_{27} = \mathbf{C}$ $Q_{28}$ $Q_{29} = \mathbf{C}$ $Q_{30} = \mathbf{C}$ $Q_{31}$
$m_0$ $m_8$ $m_4$ $m_{12}$ $m_2$ $m_{10}$ $m_6$ $m_{14}$ $m_1$ $m_9$ $m_5$ $m_{13}$ $m_3$ $m_{11}$ $m_7$ $m_{15}$
$Q_{28}$ $Q_{29} = \mathbf{C}$ $Q_{30} = \mathbf{C}$ $Q_{31}$ $Q_{32}$ $Q_{33}$ $Q_{34}$ $Q_{35}$ $Q_{36}$ $Q_{37}$ $Q_{38}$ $Q_{39}$ $Q_{40}$ $Q_{41}$ $Q_{42}$ $Q_{43}$ $Q_{44}$ $Q_{45}$ $Q_{46}$ $Q_{47}$
Initial msg
($\mathbf{C}$, $Q_{12}$, $Q_{13}$, $Q_{31}$)



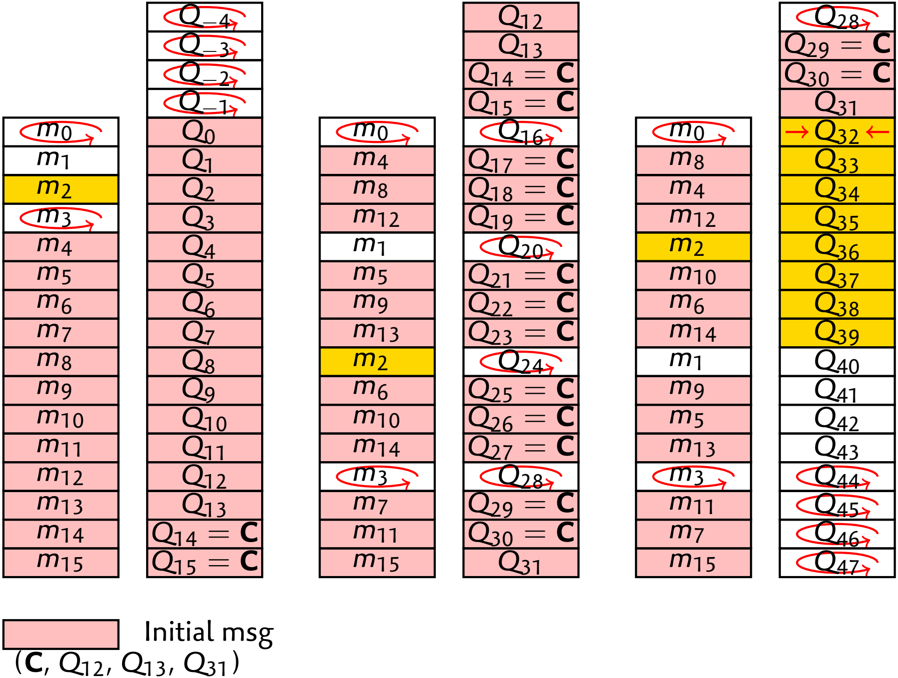
m0 m1 m2 m3 m4 m5 m6 m7 m8 m9 m10 m11 m12 m13 m14 m15
Q−4 Q−3 Q−2 Q−1 Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10 Q11 Q12 Q13 Q14 = C Q15 = C
m0 m4 m8 m12 m1 m5 m9 m13 m2 m6 m10 m14 m3 m7 m11 m15
Q12 Q13 Q14 = C Q15 = C Q16 Q17 = C Q18 = C Q19 = C Q20 Q21 = C Q22 = C Q23 = C Q24 Q25 = C Q26 = C Q27 = C Q28 Q29 = C Q30 = C Q31
m0 m8 m4 m12 m2 m10 m6 m14 m1 m9 m5 m13 m3 m11 m7 m15
Q28 Q29 = C Q30 = C Q31 Q32 Q33 Q34 Q35 Q36 Q37 Q38 Q39 Q40 Q41 Q42 Q43 Q44 Q45 Q46 Q47
Initial msg
(C, Q12, Q13, Q31)



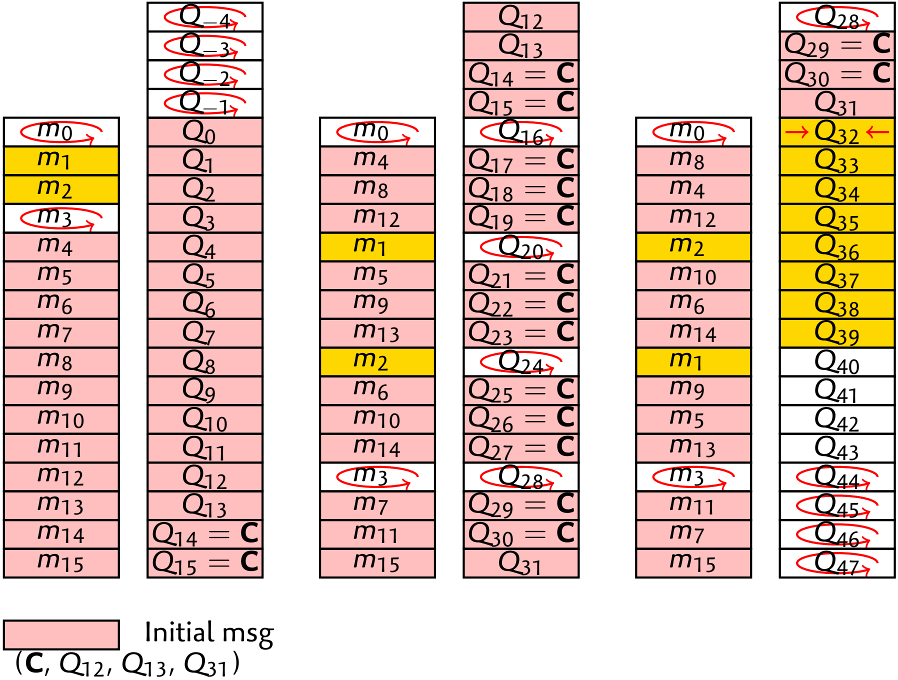
m0 m1 m2 m3 m4 m5 m6 m7 m8 m9 m10 m11 m12 m13 m14 m15
Q−4 Q−3 Q−2 Q−1 Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10 Q11 Q12 Q13
Q14 = C
Q15 = C
m0 m4 m8 m12 m1 m5 m9 m13 m2 m6 m10 m14 m3 m7 m11 m15
Q12 Q13
Q14 = C
Q15 = C
Q16
Q17 = C
Q18 = C
Q19 = C
Q20
Q21 = C
Q22 = C
Q23 = C
Q24
Q25 = C
Q26 = C
Q27 = C
Q28
Q29 = C
Q30 = C
Q31
m0 m8 m4 m12 m2 m10 m6 m14 m1 m9 m5 m13 m3 m11 m7 m15
Q28
Q29 = C
Q30 = C
Q31 Q32 Q33 Q34 Q35 Q36 Q37 Q38 Q39 Q40 Q41 Q42 Q43 Q44 Q45 Q46 Q47
Initial msg
(C, Q12, Q13, Q31)



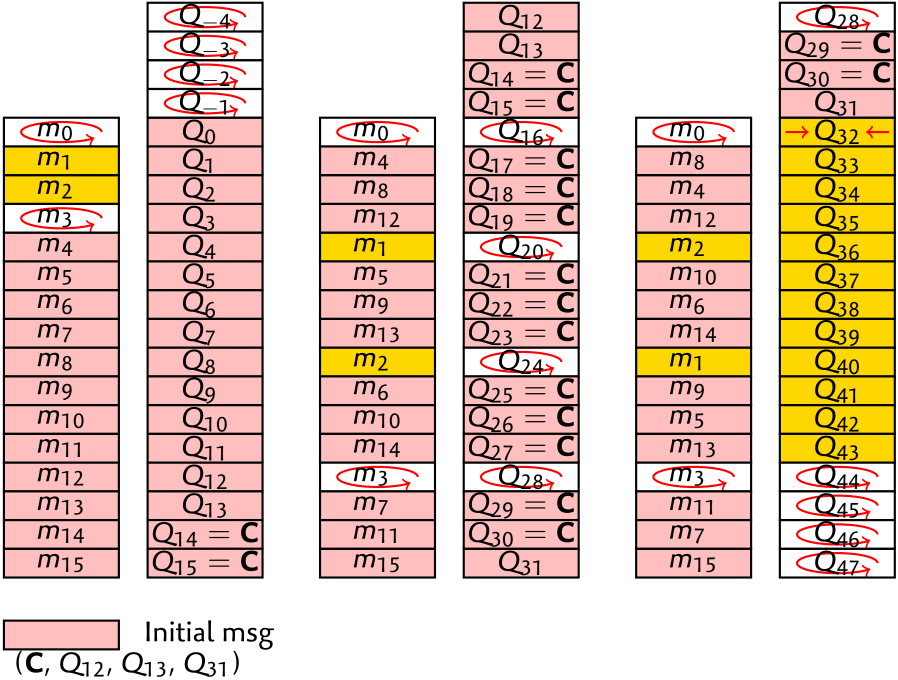
$m_0$ $m_1$ $m_2$ $m_3$ $m_4$ $m_5$ $m_6$ $m_7$ $m_8$ $m_9$ $m_{10}$ $m_{11}$ $m_{12}$ $m_{13}$ $m_{14}$ $m_{15}$
$Q_{-4}$ $Q_{-3}$ $Q_{-2}$ $Q_{-1}$ $Q_0$ $Q_1$ $Q_2$ $Q_3$ $Q_4$ $Q_5$ $Q_6$ $Q_7$ $Q_8$ $Q_9$ $Q_{10}$ $Q_{11}$ $Q_{12}$ $Q_{13}$ $Q_{14} = \mathbf{C}$ $Q_{15} = \mathbf{C}$
$m_0$ $m_4$ $m_8$ $m_{12}$ $m_1$ $m_5$ $m_9$ $m_{13}$ $m_2$ $m_6$ $m_{10}$ $m_{14}$ $m_3$ $m_7$ $m_{11}$ $m_{15}$
$Q_{12}$ $Q_{13}$ $Q_{14} = \mathbf{C}$ $Q_{15} = \mathbf{C}$ $Q_{16}$ $Q_{17} = \mathbf{C}$ $Q_{18} = \mathbf{C}$ $Q_{19} = \mathbf{C}$ $Q_{20}$ $Q_{21} = \mathbf{C}$ $Q_{22} = \mathbf{C}$ $Q_{23} = \mathbf{C}$ $Q_{24}$ $Q_{25} = \mathbf{C}$ $Q_{26} = \mathbf{C}$ $Q_{27} = \mathbf{C}$ $Q_{28}$ $Q_{29} = \mathbf{C}$ $Q_{30} = \mathbf{C}$ $Q_{31}$
$m_0$ $m_8$ $m_4$ $m_{12}$ $m_2$ $m_{10}$ $m_6$ $m_{14}$ $m_1$ $m_9$ $m_5$ $m_{13}$ $m_3$ $m_{11}$ $m_7$ $m_{15}$
$Q_{28}$ $Q_{29} = \mathbf{C}$ $Q_{30} = \mathbf{C}$ $Q_{31}$ $Q_{32}$ $Q_{33}$ $Q_{34}$ $Q_{35}$ $Q_{36}$ $Q_{37}$ $Q_{38}$ $Q_{39}$ $Q_{40}$ $Q_{41}$ $Q_{42}$ $Q_{43}$ $Q_{44}$ $Q_{45}$ $Q_{46}$ $Q_{47}$
Initial msg
($\mathbf{C}$, $Q_{12}$, $Q_{13}$, $Q_{31}$)

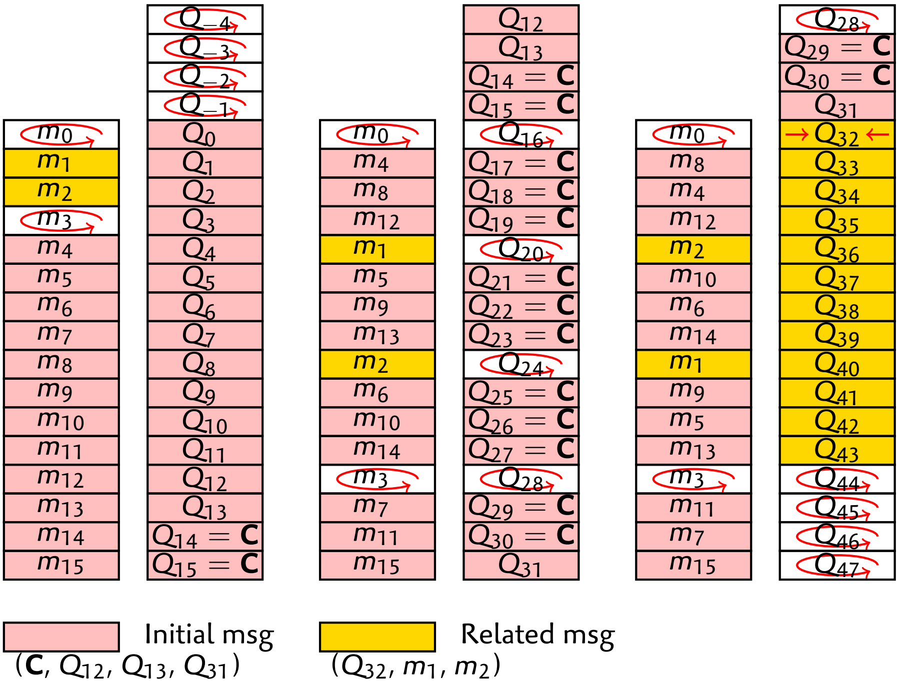


m0
m1
m2
m3
m4
m5
m6
m7
m8
m9
m10
m11
m12
m13
m14
m15
Q−4
Q−3
Q−2
Q−1
Q0
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
Q9
Q10
Q11
Q12
Q13
Q14 = C
Q15 = C
m0
m4
m8
m12
m1
m5
m9
m13
m2
m6
m10
m14
m3
m7
m11
m15
Q12
Q13
Q14 = C
Q15 = C
Q16
Q17 = C
Q18 = C
Q19 = C
Q20
Q21 = C
Q22 = C
Q23 = C
Q24
Q25 = C
Q26 = C
Q27 = C
Q28
Q29 = C
Q30 = C
Q31
m0
m8
m4
m12
m2
m10
m6
m14
m1
m9
m5
m13
m3
m11
m7
m15
Q28
Q29 = C
Q30 = C
Q31
Q32
Q33
Q34
Q35
Q36
Q37
Q38
Q39
Q40
Q41
Q42
Q43
Q44
Q45
Q46
Q47
Initial msg
(C, Q12, Q13, Q31)

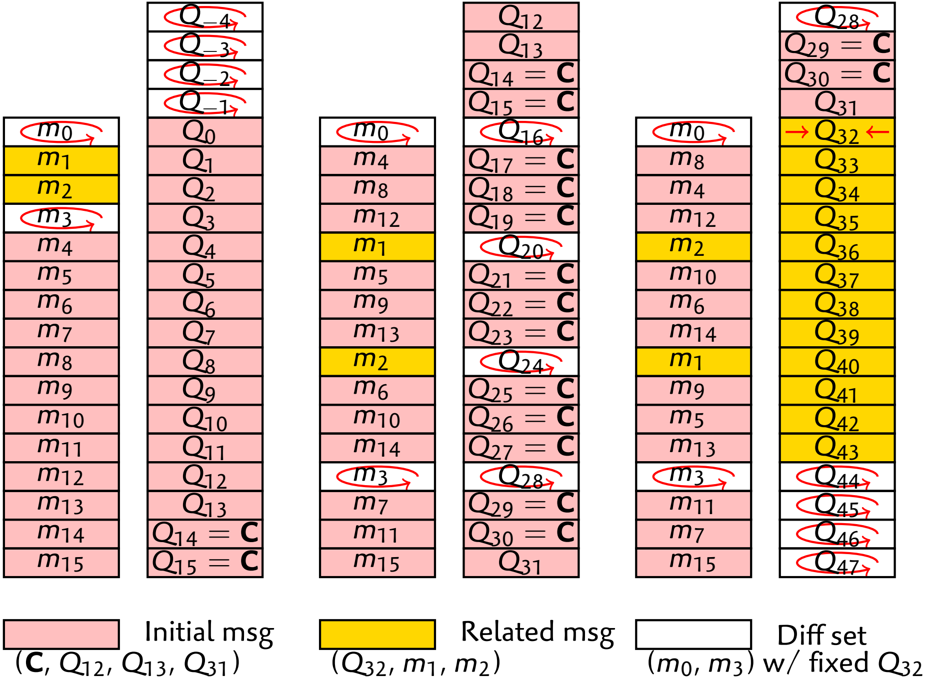


m0
m1
m2
m3
m4
m5
m6
m7
m8
m9
m10
m11
m12
m13
m14
m15
Q−4
Q−3
Q−2
Q−1
Q0
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
Q9
Q10
Q11
Q12
Q13
Q14 = C
Q15 = C
m0
m4
m8
m12
m1
m5
m9
m13
m2
m6
m10
m14
m3
m7
m11
m15
Q12
Q13
Q14 = C
Q15 = C
Q16
Q17 = C
Q18 = C
Q19 = C
Q20
Q21 = C
Q22 = C
Q23 = C
Q24
Q25 = C
Q26 = C
Q27 = C
Q28
Q29 = C
Q30 = C
Q31
m0
m8
m4
m12
m2
m10
m6
m14
m1
m9
m5
m13
m3
m11
m7
m15
Q28
Q29 = C
Q30 = C
Q31
Q32
Q33
Q34
Q35
Q36
Q37
Q38
Q39
Q40
Q41
Q42
Q43
Q44
Q45
Q46
Q47
Initial msg
(C, Q12, Q13, Q31)


$m_0$ $m_1$ $m_2$ $m_3$ $m_4$ $m_5$ $m_6$ $m_7$ $m_8$ $m_9$ $m_{10}$ $m_{11}$ $m_{12}$ $m_{13}$ $m_{14}$ $m_{15}$
$Q_{-4}$ $Q_{-3}$ $Q_{-2}$ $Q_{-1}$ $Q_0$ $Q_1$ $Q_2$ $Q_3$ $Q_4$ $Q_5$ $Q_6$ $Q_7$ $Q_8$ $Q_9$ $Q_{10}$ $Q_{11}$ $Q_{12}$ $Q_{13}$ $Q_{14} = \mathbf{C}$ $Q_{15} = \mathbf{C}$
$m_0$ $m_4$ $m_8$ $m_{12}$ $m_1$ $m_5$ $m_9$ $m_{13}$ $m_2$ $m_6$ $m_{10}$ $m_{14}$ $m_3$ $m_7$ $m_{11}$ $m_{15}$
$Q_{12}$ $Q_{13}$ $Q_{14} = \mathbf{C}$ $Q_{15} = \mathbf{C}$ $Q_{16}$ $Q_{17} = \mathbf{C}$ $Q_{18} = \mathbf{C}$ $Q_{19} = \mathbf{C}$ $Q_{20}$ $Q_{21} = \mathbf{C}$ $Q_{22} = \mathbf{C}$ $Q_{23} = \mathbf{C}$ $Q_{24}$ $Q_{25} = \mathbf{C}$ $Q_{26} = \mathbf{C}$ $Q_{27} = \mathbf{C}$ $Q_{28}$ $Q_{29} = \mathbf{C}$ $Q_{30} = \mathbf{C}$ $Q_{31}$
$m_0$ $m_8$ $m_4$ $m_{12}$ $m_2$ $m_{10}$ $m_6$ $m_{14}$ $m_1$ $m_9$ $m_5$ $m_{13}$ $m_3$ $m_{11}$ $m_7$ $m_{15}$
$Q_{28}$ $Q_{29} = \mathbf{C}$ $Q_{30} = \mathbf{C}$ $Q_{31}$ $Q_{32}$ $Q_{33}$ $Q_{34}$ $Q_{35}$ $Q_{36}$ $Q_{37}$ $Q_{38}$ $Q_{39}$ $Q_{40}$ $Q_{41}$ $Q_{42}$ $Q_{43}$ $Q_{44}$ $Q_{45}$ $Q_{46}$ $Q_{47}$
Initial msg
($\mathbf{C}$, $Q_{12}$, $Q_{13}$, $Q_{31}$)



$m_0$
$m_1$
$m_2$
$m_3$
$m_4$
$m_5$
$m_6$
$m_7$
$m_8$
$m_9$
$m_{10}$
$m_{11}$
$m_{12}$
$m_{13}$
$m_{14}$
$m_{15}$
$Q_{-4}$
$Q_{-3}$
$Q_{-2}$
$Q_{-1}$
$Q_0$
$Q_1$
$Q_2$
$Q_3$
$Q_4$
$Q_5$
$Q_6$
$Q_7$
$Q_8$
$Q_9$
$Q_{10}$
$Q_{11}$
$Q_{12}$
$Q_{13}$
$Q_{14} = \mathbf{C}$
$Q_{15} = \mathbf{C}$
$m_0$
$m_4$
$m_8$
$m_{12}$
$m_1$
$m_5$
$m_9$
$m_{13}$
$m_2$
$m_6$
$m_{10}$
$m_{14}$
$m_3$
$m_7$
$m_{11}$
$m_{15}$
$Q_{12}$
$Q_{13}$
$Q_{14} = \mathbf{C}$
$Q_{15} = \mathbf{C}$
$Q_{16}$
$Q_{17} = \mathbf{C}$
$Q_{18} = \mathbf{C}$
$Q_{19} = \mathbf{C}$
$Q_{20}$
$Q_{21} = \mathbf{C}$
$Q_{22} = \mathbf{C}$
$Q_{23} = \mathbf{C}$
$Q_{24}$
$Q_{25} = \mathbf{C}$
$Q_{26} = \mathbf{C}$
$Q_{27} = \mathbf{C}$
$Q_{28}$
$Q_{29} = \mathbf{C}$
$Q_{30} = \mathbf{C}$
$Q_{31}$
$m_0$
$m_8$
$m_4$
$m_{12}$
$m_2$
$m_{10}$
$m_6$
$m_{14}$
$m_1$
$m_9$
$m_5$
$m_{13}$
$m_3$
$m_{11}$
$m_7$
$m_{15}$
$Q_{28}$
$Q_{29} = \mathbf{C}$
$Q_{30} = \mathbf{C}$
$Q_{31}$
$Q_{32}$
$Q_{33}$
$Q_{34}$
$Q_{35}$
$Q_{36}$
$Q_{37}$
$Q_{38}$
$Q_{39}$
$Q_{40}$
$Q_{41}$
$Q_{42}$
$Q_{43}$
$Q_{44}$
$Q_{45}$
$Q_{46}$
$Q_{47}$
Initial msg
($\mathbf{C}$, $Q_{12}$, $Q_{13}$, $Q_{31}$)
Related msg
($Q_{32}$, $m_1$, $m_2$)



Initial msg
(C, $Q_{12}$, $Q_{13}$, $Q_{31}$)
Related msg
($Q_{32}$, $m_1$, $m_2$)
Diff set
($m_0$, $m_3$) w/ fixed $Q_{32}$

# Outline

# First Steps

$$Q_0 = (Q_{-4} \boxplus \mathrm{IF}(Q_{-1}, Q_{-2}, Q_{-3}) \boxplus m_0) \lll 3 \quad (1)$$
$$Q_1 = (Q_{-3} \boxplus \mathrm{IF}(Q_0, Q_{-1}, Q_{-2}) \boxplus m_1) \lll 7 \quad (2)$$
$$Q_2 = (Q_{-2} \boxplus \mathrm{IF}(Q_1, Q_0, Q_{-1}) \boxplus m_2) \lll 11 \quad (3)$$
$$Q_3 = (Q_{-1} \boxplus \mathrm{IF}(Q_2, Q_1, Q_0) \boxplus m_3) \lll 19 \quad (4)$$

- (4) gives $Q_{-1} \boxplus m_3$.
- We add the condition $Q_1 = \mathbf{1}$ to simplify (3).
- (3) gives $Q_{-2} \boxplus m_2$.
  - When $m_2$ is fixed, this gives $Q_{46} = \overline{H}_2 - Q_{-2}$.

# First Steps

$$Q_0 = (Q_{-4} \boxplus \mathrm{IF}(Q_{-1}, Q_{-2}, Q_{-3}) \boxplus m_0) \lll 3 \quad (1)$$
$$Q_1 = (Q_{-3} \boxplus \mathrm{IF}(Q_0, Q_{-1}, Q_{-2}) \boxplus m_1) \lll 7 \quad (2)$$
$$Q_2 = (Q_{-2} \boxplus \mathrm{IF}(Q_1, Q_0, Q_{-1}) \boxplus m_2) \lll 11 \quad (3)$$
$$Q_3 = (Q_{-1} \boxplus \mathrm{IF}(Q_2, Q_1, Q_0) \boxplus m_3) \lll 19 \quad (4)$$

- (4) gives $Q_{-1} \boxplus m_3$.
- We add the condition $Q_1 = \mathbf{1}$ to simplify (3).
- (3) gives $Q_{-2} \boxplus m_2$.
  - When $m_2$ is fixed, this gives $Q_{46} = \overline{H}_2 - Q_{-2}$.

# First Steps

$$Q_0 = (Q_{-4} \boxplus \text{IF}(Q_{-1}, Q_{-2}, Q_{-3}) \boxplus m_0) \lll 3 \quad (1)$$
$$Q_1 = (Q_{-3} \boxplus \text{IF}(Q_0, Q_{-1}, Q_{-2}) \boxplus m_1) \lll 7 \quad (2)$$
$$Q_2 = (Q_{-2} \boxplus \text{IF}(Q_1, Q_0, Q_{-1}) \boxplus m_2) \lll 11 \quad (3)$$
$$Q_3 = (Q_{-1} \boxplus \text{IF}(Q_2, Q_1, Q_0) \boxplus m_3) \lll 19 \quad (4)$$

- (4) gives $Q_{-1} \boxplus m_3$.
- We add the condition $Q_1 = \mathbf{1}$ to simplify (3).
- (3) gives $Q_{-2} \boxplus m_2$.
  - When $m_2$ is fixed, this gives $Q_{46} = \overline{H}_2 - Q_{-2}$.

# First Steps

$$Q_0 = (Q_{-4} \boxplus \mathrm{IF}(Q_{-1}, Q_{-2}, Q_{-3}) \boxplus m_0) \lll 3 \quad (1)$$

$$Q_1 = (Q_{-3} \boxplus \mathrm{IF}(Q_0, Q_{-1}, Q_{-2}) \boxplus m_1) \lll 7 \quad (2)$$

$$Q_2 = (Q_{-2} \boxplus \mathrm{IF}(Q_1, Q_0, Q_{-1}) \boxplus m_2) \lll 11 \quad (3)$$

$$Q_3 = (Q_{-1} \boxplus \mathrm{IF}(Q_2, Q_1, Q_0) \boxplus m_3) \lll 19 \quad (4)$$

- (4) gives $Q_{-1} \boxplus m_3$.
- We add the condition $Q_1 = \mathbf{1}$ to simplify (3).
- (3) gives $Q_{-2} \boxplus m_2$.
  - When $m_2$ is fixed, this gives $Q_{46} = \overline{H}_2 - Q_{-2}$.

# Last Steps

Let us assume that a related message $(Q_{32}, m_1, m_2)$ has been chosen. This gives $Q_{32}, \ldots Q_{43}$.

$$Q_{44} = (Q_{40} \boxplus \mathrm{XOR}(Q_{43}, Q_{42}, Q_{41}) \boxplus m_3 \boxplus K_2) \lll 3 \quad (5)$$
$$Q_{45} = (Q_{41} \boxplus \mathrm{XOR}(Q_{44}, Q_{43}, Q_{42}) \boxplus m_{11} \boxplus K_2) \lll 9 \quad (6)$$
$$Q_{46} = (Q_{42} \boxplus \mathrm{XOR}(Q_{45}, Q_{44}, Q_{43}) \boxplus m_7 \boxplus K_2) \lll 11 \quad (7)$$
$$Q_{47} = (Q_{43} \boxplus \mathrm{XOR}(Q_{46}, Q_{45}, Q_{44}) \boxplus m_{15} \boxplus K_2) \lll 15 \quad (8)$$

- (7) gives $Q_{44} \oplus Q_{45}$.
- We add the condition $Q_{41} \boxplus m_{11} \boxplus K_2 = \mathbf{0}$.
- (6) gives $Q_{45} = (Q_{45} \oplus V) \lll 9$.
  - $V = Q_{42} \oplus Q_{43} \oplus Q_{44} \oplus Q_{45}$.
  - Linear system over the bits of $Q_{43}$!

# Last Steps

Let us assume that a related message $(Q_{32}, m_1, m_2)$ has been chosen. This gives $Q_{32}, \dots Q_{43}$.

$$Q_{44} = (Q_{40} \boxplus \mathrm{XOR}(Q_{43}, Q_{42}, Q_{41}) \boxplus m_3 \boxplus K_2) \lll 3 \quad (5)$$

$$Q_{45} = (Q_{41} \boxplus \mathrm{XOR}(Q_{44}, Q_{43}, Q_{42}) \boxplus m_{11} \boxplus K_2) \lll 9 \quad (6)$$

$$Q_{46} = (Q_{42} \boxplus \mathrm{XOR}(Q_{45}, Q_{44}, Q_{43}) \boxplus m_7 \boxplus K_2) \lll 11 \quad (7)$$

$$Q_{47} = (Q_{43} \boxplus \mathrm{XOR}(Q_{46}, Q_{45}, Q_{44}) \boxplus m_{15} \boxplus K_2) \lll 15 \quad (8)$$

- (7) gives $Q_{44} \oplus Q_{45}$.
- We add the condition $Q_{41} \boxplus m_{11} \boxplus K_2 = \mathbf{0}$.
- (6) gives $Q_{45} = (Q_{45} \oplus V) \lll 9$.
  - $V = Q_{42} \oplus Q_{43} \oplus Q_{44} \oplus Q_{45}$.
  - Linear system over the bits of $Q_{43}$!

# Last Steps

Let us assume that a related message $(Q_{32}, m_1, m_2)$ has been chosen. This gives $Q_{32}, \ldots Q_{43}$.

$$Q_{44} = (Q_{40} \boxplus \mathrm{XOR}(Q_{43}, Q_{42}, Q_{41}) \boxplus m_3 \boxplus K_2) \lll 3 \quad (5)$$

$$Q_{45} = (Q_{41} \boxplus \mathrm{XOR}(Q_{44}, Q_{43}, Q_{42}) \boxplus m_{11} \boxplus K_2) \lll 9 \quad (6)$$

$$Q_{46} = (Q_{42} \boxplus \mathrm{XOR}(Q_{45}, Q_{44}, Q_{43}) \boxplus m_7 \boxplus K_2) \lll 11 \quad (7)$$

$$Q_{47} = (Q_{43} \boxplus \mathrm{XOR}(Q_{46}, Q_{45}, Q_{44}) \boxplus m_{15} \boxplus K_2) \lll 15 \quad (8)$$

- (7) gives $Q_{44} \oplus Q_{45}$.
- We add the condition $Q_{41} \boxplus m_{11} \boxplus K_2 = \mathbf{0}$.
- (6) gives $Q_{45} = (Q_{45} \oplus V) \lll 9$.
  - $V = Q_{42} \oplus Q_{43} \oplus Q_{44} \oplus Q_{45}$.
  - Linear system over the bits of $Q_{43}$!

# Last Steps

Let us assume that a related message $(Q_{32}, m_1, m_2)$ has been chosen.
This gives $Q_{32}, \dots Q_{43}$.

$$Q_{44} = (Q_{40} \boxplus \text{XOR}(Q_{43}, Q_{42}, Q_{41}) \boxplus m_3 \boxplus K_2) \lll 3 \qquad (5)$$

$$Q_{45} = (Q_{41} \boxplus \text{XOR}(Q_{44}, Q_{43}, Q_{42}) \boxplus m_{11} \boxplus K_2) \lll 9 \qquad (6)$$

$$Q_{46} = (Q_{42} \boxplus \text{XOR}(Q_{45}, Q_{44}, Q_{43}) \boxplus m_7 \boxplus K_2) \lll 11 \qquad (7)$$

$$Q_{47} = (Q_{43} \boxplus \text{XOR}(Q_{46}, Q_{45}, Q_{44}) \boxplus m_{15} \boxplus K_2) \lll 15 \qquad (8)$$

- (7) gives $Q_{44} \oplus Q_{45}$.
- We add the condition $Q_{41} \boxplus m_{11} \boxplus K_2 = \mathbf{0}$.
- (6) gives $Q_{45} = (Q_{45} \oplus V) \lll 9$.
  - $V = Q_{42} \oplus Q_{43} \oplus Q_{44} \oplus Q_{45}$.
  - Linear system over the bits of $Q_{43}$!

# Extra Conditions

We have introduced two extra conditions:

1. $Q_1 = \mathbf{1}$
   Can be satisfied statistically by the initial message.

2. $Q_{41} \oplus m_{11} \oplus K_2 = \mathbf{0}$
   Can be satisfied by a good choice of $m_1$, after $m_2$ has been fixed:

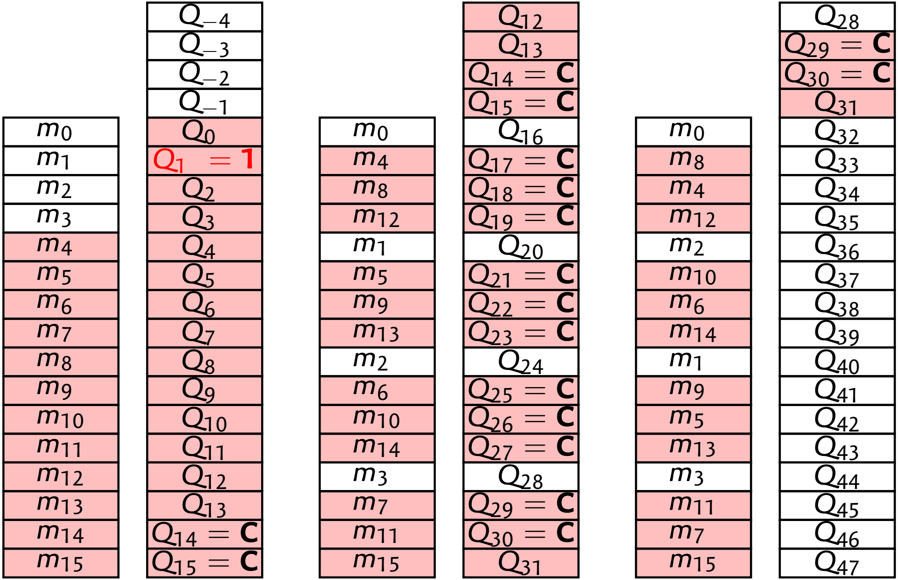
$$Q_{40} = (Q_{36} \boxplus \mathrm{XOR}(Q_{39}, Q_{38}, Q_{37}) \boxplus m_1 \boxplus K_2) \lll 3 \qquad (9)$$

$$Q_{41} = (Q_{37} \boxplus \mathrm{XOR}(Q_{40}, Q_{39}, Q_{38}) \boxplus m_9 \boxplus K_2) \lll 3 \qquad (10)$$

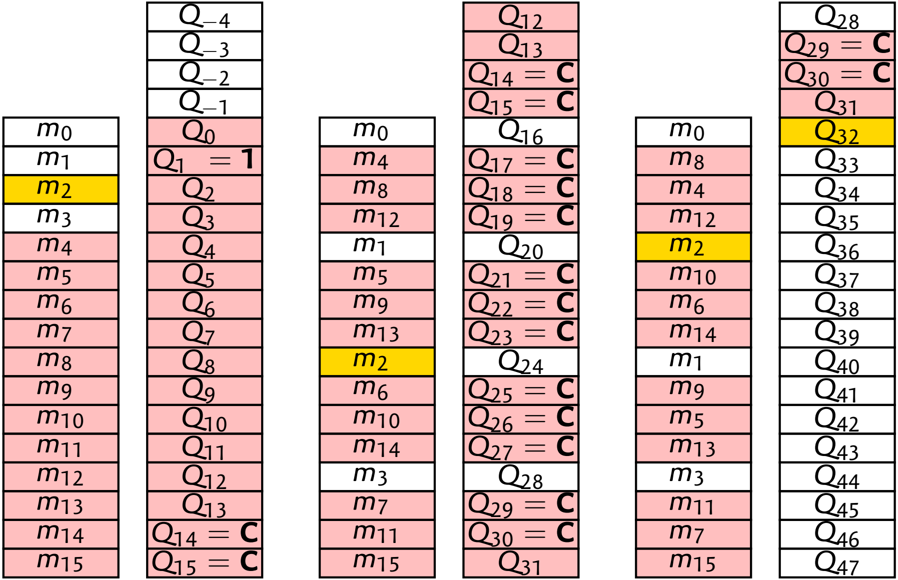
- The condition gives $Q_{41}$.
- (10) gives $Q_{40}$.
- (9) gives $m_1$.

# Result

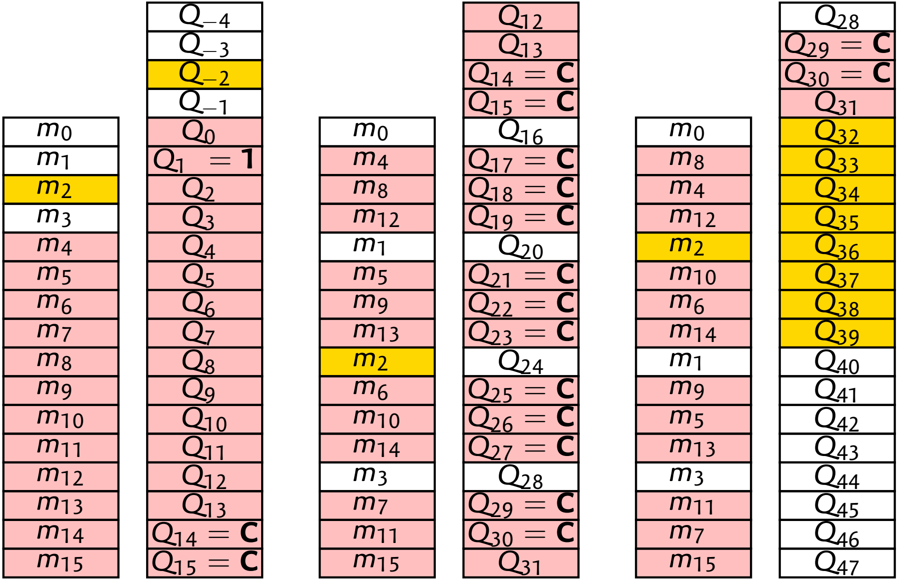
- For a well chosen initial message and a well chosen related message, if we assume that $\overline{H}$ is in the differential set, we can find the right message in time 1.
- So we can test whether $\overline{H}$ is in the related set in time 1.
- The cost of finding a good initial message is amortized over many good related messages.



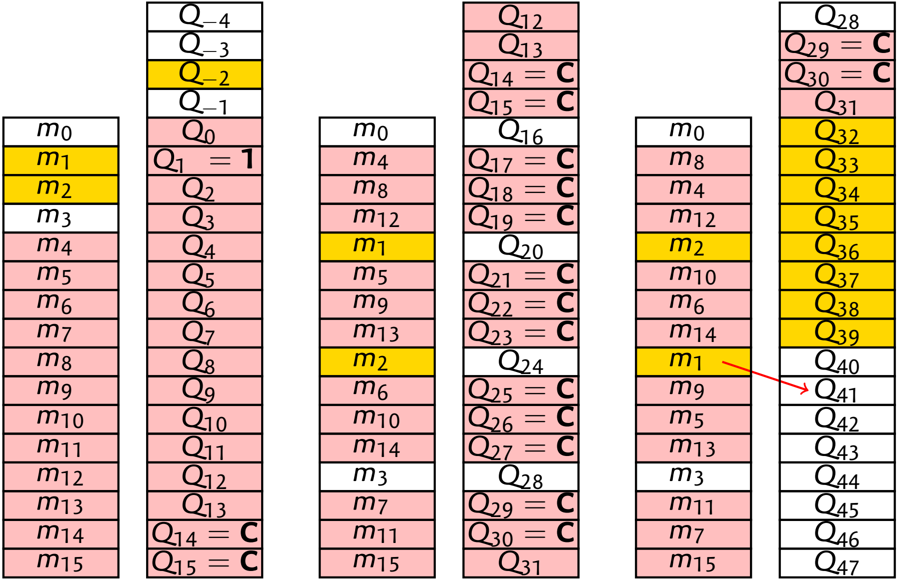

1: Choose an initial message with $Q_1 = \mathbf{1}$



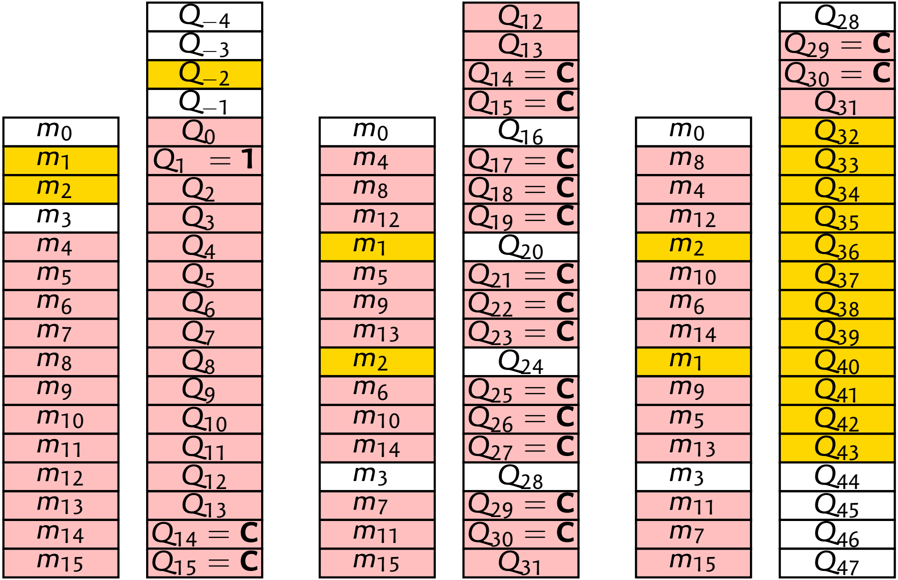

2: **for all** $Q_{32}, m_2$ **do**



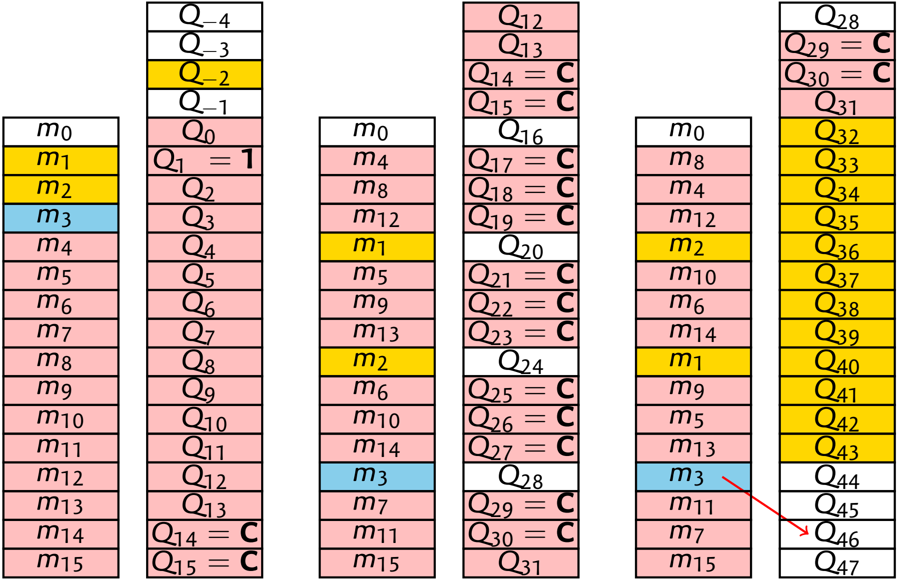

2: **for all** $Q_{32}, m_2$ **do**



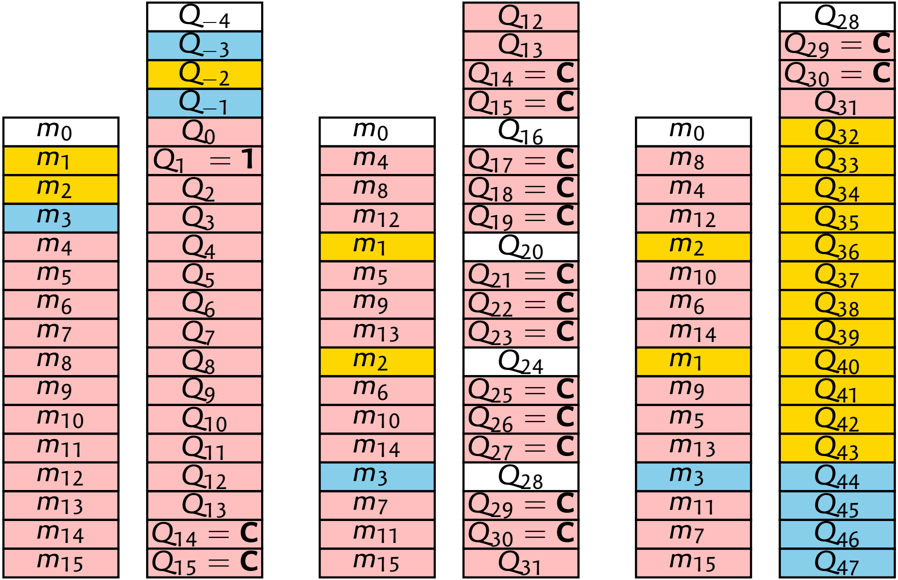

3: Choose $m_1$ s.t. $Q_{41} = -m_{11} - K_2$.



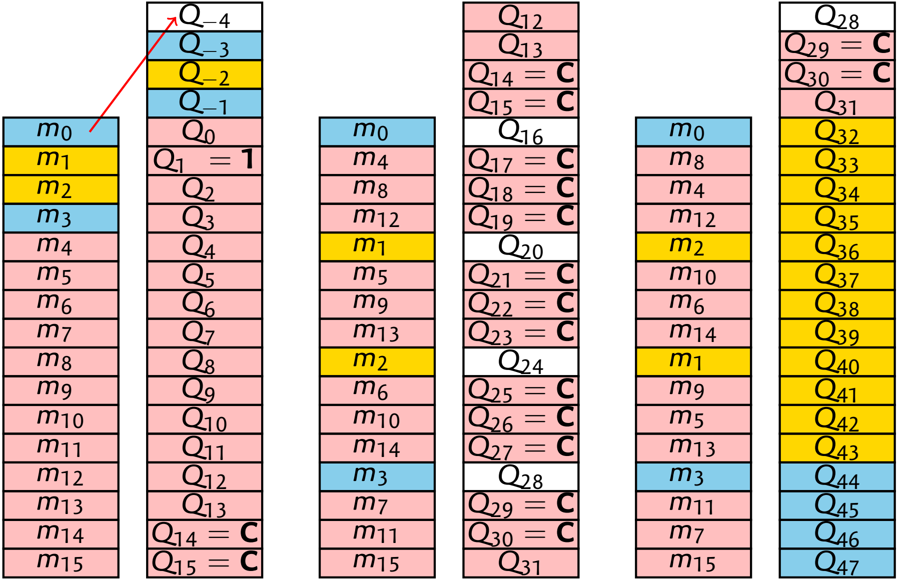

3: Choose $m_1$ s.t. $Q_{41} = -m_{11} - K_2$.




4: Choose $m_3$ s.t. $Q_{46} = \overline{H}_2 \boxminus Q_{-2}$.



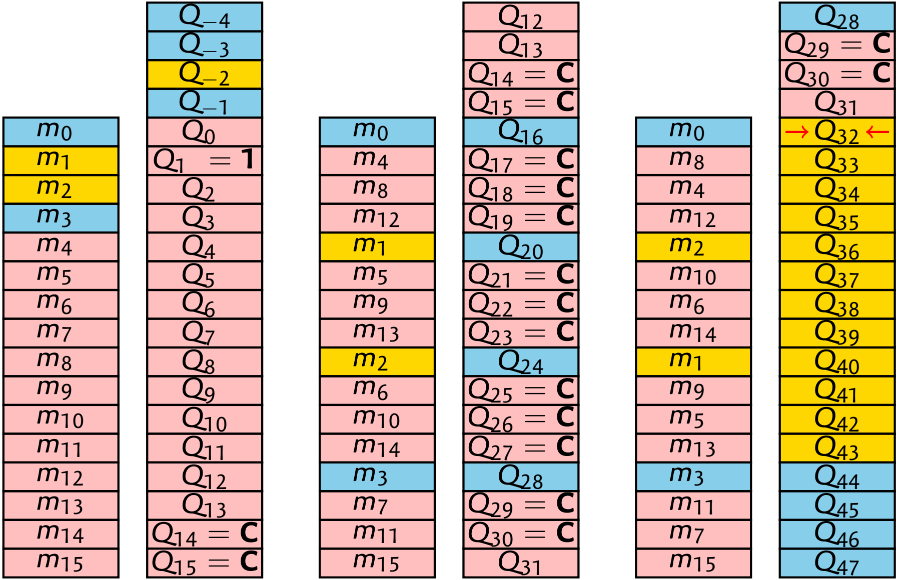

4: Choose $m_3$ s.t. $Q_{46} = \overline{H}_2 \boxminus Q_{-2}$.




5: Choose $m_0$ s.t. $Q_{-4} = \overline{H}_0 \boxminus Q_{44}$.

| | | | | | |
|---|---|---|---|---|---|
| | $Q_{-4}$ | | $Q_{12}$ | | $Q_{28}$ |
| | $Q_{-3}$ | | $Q_{13}$ | | $Q_{29} = \mathbf{C}$ |
| | $Q_{-2}$ | | $Q_{14} = \mathbf{C}$ | | $Q_{30} = \mathbf{C}$ |
| | $Q_{-1}$ | | $Q_{15} = \mathbf{C}$ | | $Q_{31}$ |
| $m_0$ | $Q_0$ | $m_0$ | $Q_{16}$ | $m_0$ | $Q_{32}$ |
| $m_1$ | $Q_1 = \mathbf{1}$ | $m_4$ | $Q_{17} = \mathbf{C}$ | $m_8$ | $Q_{33}$ |
| $m_2$ | $Q_2$ | $m_8$ | $Q_{18} = \mathbf{C}$ | $m_4$ | $Q_{34}$ |
| $m_3$ | $Q_3$ | $m_{12}$ | $Q_{19} = \mathbf{C}$ | $m_{12}$ | $Q_{35}$ |
| $m_4$ | $Q_4$ | $m_1$ | $Q_{20}$ | $m_2$ | $Q_{36}$ |
| $m_5$ | $Q_5$ | $m_5$ | $Q_{21} = \mathbf{C}$ | $m_{10}$ | $Q_{37}$ |
| $m_6$ | $Q_6$ | $m_9$ | $Q_{22} = \mathbf{C}$ | $m_6$ | $Q_{38}$ |
| $m_7$ | $Q_7$ | $m_{13}$ | $Q_{23} = \mathbf{C}$ | $m_{14}$ | $Q_{39}$ |
| $m_8$ | $Q_8$ | $m_2$ | $Q_{24}$ | $m_1$ | $Q_{40}$ |
| $m_9$ | $Q_9$ | $m_6$ | $Q_{25} = \mathbf{C}$ | $m_9$ | $Q_{41}$ |
| $m_{10}$ | $Q_{10}$ | $m_{10}$ | $Q_{26} = \mathbf{C}$ | $m_5$ | $Q_{42}$ |
| $m_{11}$ | $Q_{11}$ | $m_{14}$ | $Q_{27} = \mathbf{C}$ | $m_{13}$ | $Q_{43}$ |
| $m_{12}$ | $Q_{12}$ | $m_3$ | $Q_{28}$ | $m_3$ | $Q_{44}$ |
| $m_{13}$ | $Q_{13}$ | $m_7$ | $Q_{29} = \mathbf{C}$ | $m_{11}$ | $Q_{45}$ |
| $m_{14}$ | $Q_{14} = \mathbf{C}$ | $m_{11}$ | $Q_{30} = \mathbf{C}$ | $m_7$ | $Q_{46}$ |
| $m_{15}$ | $Q_{15} = \mathbf{C}$ | $m_{15}$ | $Q_{31}$ | $m_{15}$ | $Q_{47}$ |

5: Choose $m_0$ s.t. $Q_{-4} = \overline{H}_0 \boxminus Q_{44}$.




**if** $m_0$ matches $Q_{32}$ **then**

  **return**

# Partial Pseudo Preimage Algorithm

**Input:** $\overline{H}_0, \overline{H}_2$
**Output:** $M$, IV st. $H_0 = \overline{H}_0$, $H_2 = \overline{H}_2$
**Running Time:** $2^{32}$

```
loop                                                  ▷ We expect 1 iteration
    Choose an initial msg. with Q_1 = 1               ▷ 2^96 possibilities
    for all Q_32, m_2 do                              ▷ 2^32 iterations

        Choose m_1 s.t. Q_41 = −m_11 − K_2.
        Choose m_3 s.t. Q_46 = H̄_2 ⊟ Q_−2.            ▷ Q_46 ⊞ Q_−2 is H_2
        Choose m_0 s.t. Q_−4 = H̄_0 ⊟ Q_44.            ▷ Q_44 ⊞ Q_−4 is H_0
        if m_0 matches Q_32 then                      ▷ OK with probability 2^−32
            return
```

- We run this $2^{64}$ times for a full pseudo-preimage: complexity $2^{96}$
- We can also choose $\mathrm{IV}_2$!

# Partial Pseudo Preimage Algorithm

**Input:** $\overline{H}_0, \overline{H}_2, \overline{\mathrm{IV}}_2$
**Output:** $M$, IV st. $H_0 = \overline{H}_0$, $H_2 = \overline{H}_2$ and $\mathrm{IV}_2 = \overline{\mathrm{IV}}_2$
**Running Time:** $2^{32}$

**loop** ▷ *We expect 1 iteration*
  Choose an initial msg. with $Q_1 = \mathbf{1}$ ▷ $2^{96}$ *possibilities*
  **for all** $Q_{32}$ **do** ▷ $2^{32}$ *iterations*
    Choose $m_2$ s.t. $Q_{-2} = \overline{\mathrm{IV}}_2$. ▷ $Q_{-2}$ *is* $\mathrm{IV}_2$
    Choose $m_1$ s.t. $Q_{41} = -m_{11} - K_2$.
    Choose $m_3$ s.t. $Q_{46} = \overline{H}_2 \boxminus Q_{-2}$. ▷ $Q_{46} \boxplus Q_{-2}$ *is* $H_2$
    Choose $m_0$ s.t. $Q_{-4} = \overline{H}_0 \boxminus Q_{44}$. ▷ $Q_{44} \boxplus Q_{-4}$ *is* $H_0$
    **if** $m_0$ matches $Q_{32}$ **then** ▷ *OK with probability* $2^{-32}$
      **return**

- We run this $2^{64}$ times for a full pseudo-preimage: complexity $2^{96}$
- We can also choose $\mathrm{IV}_2$!

# Outline

# The Padding Block

- We have to put the padding inside a preimage block.
- We use a message of $512b - 65$ bits ($b$ blocks).
- Extra conditions:
  - $m_{15} = 0$.
    $\rightarrow$ easy: we choose $m_{15}$.
  - $m_{14} =$ msg. size.

$$Q_{27} = (Q_{23} \boxplus \mathrm{MAJ}(Q_{26}, Q_{25}, Q_{24}) \boxplus m_{14} \boxplus K_1) \lll 13$$
$$m_{14} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1$$

  - The message is padded with a single 1 followed by 0's.

$$\mathbf{C} = (\mathbf{C} \boxplus \mathbf{C} \boxplus m_{13} \boxplus K_1) \lll 13$$
$$m_{13} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1 = m_{14}$$

# The Padding Block

- We have to put the padding inside a preimage block.
- We use a message of $512b - 65$ bits ($b$ blocks).
- Extra conditions:
  - $m_{15} = 0$.
    $\rightarrow$ easy: we choose $m_{15}$.
  - $m_{14} =$ msg. size.

$$Q_{27} = (Q_{23} \boxplus \mathrm{MAJ}(Q_{26}, Q_{25}, Q_{24}) \boxplus m_{14} \boxplus K_1) \lll 13$$
$$m_{14} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1$$

  - The message is padded with a single 1 followed by 0's.

$$\mathbf{C} = (\mathbf{C} \boxplus \mathbf{C} \boxplus m_{13} \boxplus K_1) \lll 13$$
$$m_{13} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1 = m_{14}$$

# The Padding Block

- We have to put the padding inside a preimage block.
- We use a message of $512b - 65$ bits ($b$ blocks).
- Extra conditions:
  - $m_{15} = 0$.
    $\rightarrow$ easy: we choose $m_{15}$.
  - $m_{14} = 512b - 65$.

$$Q_{27} = (Q_{23} \boxplus \mathrm{MAJ}(Q_{26}, Q_{25}, Q_{24}) \boxplus m_{14} \boxplus K_1) \lll 13$$
$$m_{14} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1$$

  - $m_{13}^{[0]} = 1$.

$$\mathbf{C} = (\mathbf{C} \boxplus \mathbf{C} \boxplus m_{13} \boxplus K_1) \lll 13$$
$$m_{13} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1 = m_{14}$$

# The Padding Block

- We have to put the padding inside a preimage block.
- We use a message of $512b - 65$ bits ($b$ blocks).
- Extra conditions:
  - $m_{15} = 0$.
    $\rightarrow$ easy: we choose $m_{15}$.
  - $m_{14} = 512b - 65$.

$$Q_{27} = (Q_{23} \boxplus \mathrm{MAJ}(Q_{26}, Q_{25}, Q_{24}) \boxplus m_{14} \boxplus K_1) \lll 13$$
$$m_{14} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1$$

  - $m_{13}^{[0]} = 1$.

$$\mathbf{C} = (\mathbf{C} \boxplus \mathbf{C} \boxplus m_{13} \boxplus K_1) \lll 13$$
$$m_{13} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1 = m_{14}$$

# The Padding Block

- We have to put the padding inside a preimage block.
- We use a message of $512b - 65$ bits ($b$ blocks).
- Extra conditions:
  - $m_{15} = 0$.
    $\rightarrow$ easy: we choose $m_{15}$.
  - $m_{14} = 512b - 65$.

$$Q_{27} = (Q_{23} \boxplus \mathrm{MAJ}(Q_{26}, Q_{25}, Q_{24}) \boxplus m_{14} \boxplus K_1) \lll 13$$

$$m_{14} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1$$

  - $m_{13}^{[0]} = 1$.

$$\mathbf{C} = (\mathbf{C} \boxplus \mathbf{C} \boxplus m_{13} \boxplus K_1) \lll 13$$

$$m_{13} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1 = m_{14}$$

# The Padding Block

- We have to put the padding inside a preimage block.
- We use a message of $512b - 65$ bits ($b$ blocks).
- Extra conditions:
  - $m_{15} = 0$.
    $\rightarrow$ easy: we choose $m_{15}$.
  - $m_{14} = 512b - 65$.

$$\mathbf{C} = ( \mathbf{C} \boxplus \mathbf{C} \boxplus m_{14} \boxplus K_1 ) \lll 13$$

$$m_{14} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1$$

  - $m_{13}^{[0]} = 1$.

$$\mathbf{C} = (\mathbf{C} \boxplus \mathbf{C} \boxplus m_{13} \boxplus K_1) \lll 13$$

$$m_{13} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1 = m_{14}$$

# The Padding Block

- We have to put the padding inside a preimage block.
- We use a message of $512b - 65$ bits ($b$ blocks).
- Extra conditions:
  - $m_{15} = 0$.
    $\longrightarrow$ easy: we choose $m_{15}$.
  - $m_{14} = 512b - 65$.

$$\mathbf{C} = (\mathbf{C} \boxplus \mathbf{C} \boxplus m_{14} \boxplus K_1) \lll 13$$
$$m_{14} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1$$

  - $m_{13}^{[0]} = 1$.

$$\mathbf{C} = (\mathbf{C} \boxplus \mathbf{C} \boxplus m_{13} \boxplus K_1) \lll 13$$
$$m_{13} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1 = m_{14}$$

# The Padding Block

- We have to put the padding inside a preimage block.
- We use a message of $512b - 65$ bits ($b$ blocks).
- Extra conditions:
  - $m_{15} = 0$.
    $\rightarrow$ easy: we choose $m_{15}$.
  - $m_{14} = 512b - 65$.

$$\mathbf{C} = (\ \mathbf{C} \boxplus \qquad \mathbf{C} \qquad \boxplus m_{14} \boxplus K_1) \lll 13$$
$$m_{14} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1$$

  - $m_{13}^{[0]} = 1$.

$$\mathbf{C} = (\mathbf{C} \boxplus \mathbf{C} \boxplus m_{13} \boxplus K_1) \lll 13$$
$$m_{13} = \mathbf{C} \ggg 13 \boxminus \mathbf{C} \boxminus \mathbf{C} \boxminus K_1 = m_{14}$$

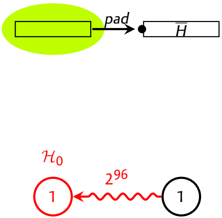
# Improved meet-in-the-middle

- The pseudo-preimage attack has complexity $2^{96}$
- The generic meet-in-the-middle attack has complexity $2^{113}$
- Our pseudo-preimage attack has a special property:
  We can target a set of size $2^k$ with complexity $2^{96-k}$

# Layered Hash Tree

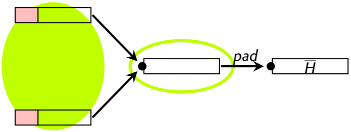

- Start with $\bar{H}$.
- Compute a padding block.
- Double the set size.
- Meet in the middle.

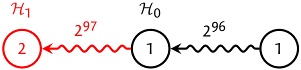
# Layered Hash Tree




- Start with $\bar{H}$.
- Compute a padding block.
- Double the set size.
- Meet in the middle.

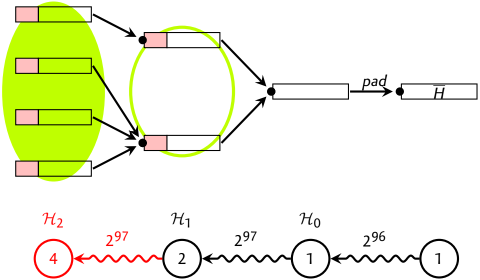
# Layered Hash Tree



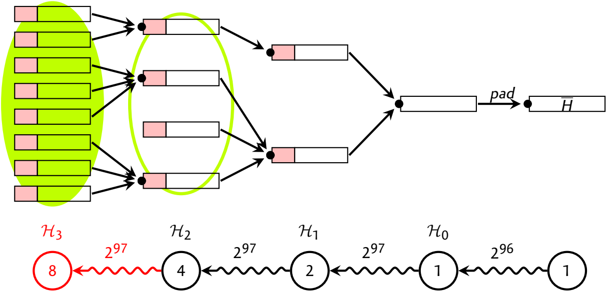

- Start with $\bar{H}$.
- Compute a padding block.
- Double the set size.
- Meet in the middle.

# Layered Hash Tree



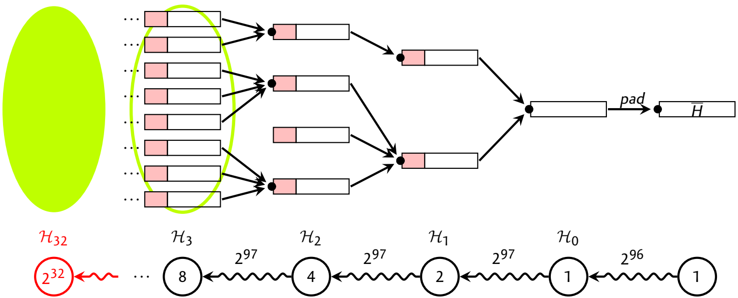

- Start with $\bar{H}$.
- Compute a padding block.
- Double the set size. (iterate)
- Meet in the middle.

# Layered Hash Tree



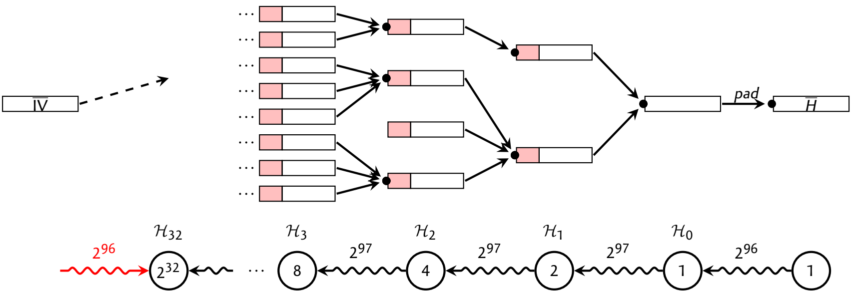

- Start with $\bar{H}$.
- Compute a padding block.
- Double the set size. (iterate)
- Meet in the middle.

# Layered Hash Tree




- Start with $\bar{H}$.
- Compute a padding block.
- Double the set size. (iterate)
- Meet in the middle.

# Layered Hash Tree




- Start with $\bar{H}$.
- Compute a padding block.
- Double the set size. (iterate)
- Meet in the middle.

# Summary of our results

- We use differential tools to find pseudo-preimages.
- We have just enough freedom to include the padding.
- We use some specific properties of our pseudo-preimages to improve the meet-in-the-middle.

### The preimage attack

- Time complexity: $2^{102}$
- Memory: $2^{32}$
- Preimage length is about 20 blocks.

# Any Questions?

*Thank you for your attention.*

# Future Work

*Application to MD5? SHA?*

Quite unlikely...

- The round functions can't absorb a difference
- More rounds
- Better message expansion in SHA

# Future Work

## *Practical impact?*

Some constructions use a truncated MD4 (S/KEY, rsync), but:

- Our attack only works if $H_2$ is part of the output
- We can't do a meet-in-the-middle in less than $2^{64}$

We did not find a "bad enough" construction.